

Perle 1700 Series

Bridge / Routers With VPN User And System Administration Guide

Part number 5500074-16

Encryption product delivery, import and use

Delivery of Perle cryptographic products does not imply third-party authority to import, distribute, or use encryption. Importers, distributors, and users are responsible for compliance with all local country laws. Perle strongly recommends that importers, distributors, and users investigate such regulations prior to encryption product deployment.

Federal Communications Commission (FCC)

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Warning: The user is cautioned that modifications to this equipment can void the authority granted by the FCC to operate the equipment

The following repairs may be made by the customer: none.

Canadian Emissions Standard ICES-003

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus", ICES-003 of the Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par Industrie Canada.

For products marked with the CE Telecommunications label, the following declaration applies:

"The manufacturer declares that as shipped from the factory this product is in compliance with the CE Telecommunications Terminal Equipment Directive 91/263/EEC with the marking **CE 168 X** applied in respect of this declaration, and in respect of the following telecommunications interfaces,

X.21(V.11) - NET 1

X.21bis(V.28) and X.21bis(V.35) - NET 2

PSTN ISDN Basic Rate Interface compatible with I.420 - NET 3

The manufacturer further declares that the product conforms with the requirements of the Low Voltage Directive 73/23/EEC and with the requirements of the EMC Directive 89/336/EEC (for radiated emissions at the Class A level). This product is not intended for residential applications."

ISDN Type Approval Labels

Labels for National ISDN Type Approvals can be found on the inside surface of the backpanel of the ISDN module.

Canadian ISDN Approval

The ISDN interface of this device is intended for direct connection to the S/T jack of an NT-1 unit and therefore does not require Communications Canada certification. The P1730 & PRO should only be connected to Communications Canada approved NT-1 units.

Statements for ISDN U Module

NOTICE: The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunication company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alteration made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Using This Manual

This Installation and Applications Guide provides the basic information required to initially set-up and configure the P1730 & PRO Bridge/Router. This guide is organized into the following sections:

“**Installation**” provides instructions for installing the P1730 & P1705.

“**Typical Applications & How to Configure Them**” provides simple configuration examples for typical applications in which the P1705 & P1730 might be used. The applications described in this document are for example only and provide a method of quick configuration of the P1705 & P1730. The applications and corresponding configuration may be combined if the operation of the P1705 & P1730 requires more complexity. For more complete information on all of the configuration parameters available please refer to the appropriate Menu Reference Manual file for your operating software on the accompanying CD-ROM.

“**Introduction to Filtering**” provides an introduction to the pattern filtering options of the P1705 & P1730. Several examples of typical pattern filters are also provided.

“**Menu Trees**” provides a graphical tree type overview of the structure of the built-in menu system of the P1705 & P1730. All of the configuration is performed using the options provided in the menu system. The Menu Tree is like an index to the menu options.

“**Octet Locations on Ethernet Frames**” provides a graphical representation of the various common Ethernet frames that the P1705 & P1730 will bridge or route. When defining a pattern filter, these frame displays indicate the offset values to use in order to define the pattern filter correctly.

“**Servicing Information**” provides information on changing Link interfaces.

“**Interface Pinouts**” provides information on Link interface connectors.

Using The Electronic Reference Manuals

This manual and the P1705 & P1730 Reference Manuals are provided as Adobe Acrobat PDF files on the accompanying CD-ROM.

The Adobe Acrobat Reader program required to view the Manuals is also loaded onto the CD-ROM. In addition, it is available for most computer operating platforms from Adobe on the Internet at: www.adobe.com.

The Reference Manual provides the following information:

- Introduction to bridging, routing, and P1705 & P1730 features,
- Pin out references for the link modules,
- List of event and alarm logs, and
- Expanded description of programmable filtering.

The PPP Menu Reference Manual provides the following information:

- Complete description of the options for the built-in menu system, including PPP ISDN, PPP Leased Line, 1490 Frame Relay and encapsulated PPP Frame Relay.

1	INSTALLATION	1
	Unpack the Router.....	1
	Select a Site	1
	Identify the Reset Switch	2
	Identify the Connectors	3
	P1705.....	3
	P1730.....	3
	Connect to the Console.....	4
	Make the Link Connection(s).....	4
	Power Up the Bridge/Router.....	5
	Managing the P1705 & P1730 Using the Menus	5
	Conventions.....	6
	Login to Bridge/Router and Enter the Required Configuration.....	7
	Mandatory Configuration.....	8
	Setting the T1/E1Parameters (T1/E1 WAN only)	9
	Identify the Status LEDs	11
2	TYPICAL APPLICATIONS & HOW TO CONFIGURE THEM	12
	Bridging and Routing	13
	Should You Bridge or Route?	13
	Bridging.....	14
	IP Routing	15
	IP Addressing.....	16
	Masks	17
	IP Subnets.....	17
	IP Default Gateway.....	19
	IP Static Route	19
	IPX Routing	20
	Novell Servers in Both Locations.....	20
	Novell Servers in One Location Only	21
	Novell Server with Dual LANs.....	23
	PPP Overview.....	24
	PPP Link Configuration.....	24
	Numbered Links.....	24
	Unnumbered Links	25
	Multilink Operation.....	26
	Basic WAN Configurations.....	27
	Basic ISDN Connections.....	27
	PPP ISDN Manual Call Quick Connections.....	29
	IPX Router Manual Call Connection	30
	IP Router Manual Call Connection	30
	Basic Frame Relay Configuration	31
	Auto Learning the Frame Relay Configuration.....	32
	Manual Configuration - LMI Type.....	33
	Quick Start Frame Relay	34
	Basic Leased Line Configuration	35
	Quick Start PPP Leased Line Connections	35
	Bridge Connection.....	36
	IP Router Connection.....	36
	IPX Router Connection.....	36

Contents

Configure Remote Site Profiles	37
Configure Remote Site Profiles for ISDN PPP	38
Configure Remote Site Profile for Frame Relay	40
Configure Remote Site Profiles for Leased Line PPP	43
Configure Remote Site Profiles for Frame Relay with ISDN backup	45
Configure Remote Site Profiles for PPPoE.....	46
Advanced Features	50
Configure Dynamic Host Configuration Protocol	50
Network Address Translation and Port Translation.....	52
Security.....	54
IPSec Protocol Suite.....	54
Internet Key Exchange (IKE).....	61
Configure PPP Security.....	64
Configure Firewall.....	66
Network Address Translation.....	69
Filters.....	69
Compression	69
Bandwidth On Demand.....	70
QOS - Priority Queuing.....	71
Simple Network Time Protocol (SNTP).....	73
3 INTRODUCTION TO FILTERING	75
MAC Address Filtering.....	75
Pattern Filtering.....	75
Popular Filters	77
Bridge	77
IP & Related Traffic.....	77
Novell IPX Frames	77
NetBIOS &NetBEUI (Windows For Workgroups)	77
Banyan.....	77
IP Router.....	78
NetBIOS over TCP	78
Other interesting TCP Ports	78
APPENDIX A MENU TREES	79
APPENDIX B OCTET LOCATIONS ON ETHERNET FRAMES	84
Octet Locations on a Bridged TCP/IP Frame.....	84
Octet Locations on a Bridged Novell Netware Frame	85
ETHERNET Type Codes	85
Octet Locations on an IP Routed TCP/IP Frame.....	86
Octet Locations on an IPX Routed Novell Netware Frame	86
Octet Locations on a Bridged XNS Frame	87
APPENDIX C SERVICING INFORMATION	88
Opening the case	88
Identifying the Internal Components	89
To Clear a “Lost” Password	90
Changing LAN or WAN Interfaces.....	90
Selecting MDI or MDI-X LAN Interface.....	90

Installing the ISDN Link Modules	91
Processor settings for the ISDN Link Modules	91
Changing the Termination Straps on the ISDN S/T Interface	92
Connecting to the ISDN-U Link Module	92
Performing a Software Upgrade	93
APPENDIX D INTERFACE PINOUTS	95
Pinout Information	95
Link Clocking Information	95
ATL-CSU/DSU Link Module Information	95
Console Pinouts	97
T1/E1 Module:	98
V.24 & RS232C Link Pinouts	99
V.11/X.21 Link Pinouts	100
RS442 & RS530 Link Pinouts	101
V.35 Link Pinouts	102
RS232 Null-Modem Cable Configuration	103
V.35 Null-Modem Cable Configuration	104
RS530 Null-Modem Cable Configuration	105
RS530 To RS449 Conversion Cable	106
V.11/X.21 Null-Modem Cable Configuration	107

I

Installation

The P1705 & P1730 are flexible Ethernet Bridge/Routers that may be configured to service Local Area Networks and Wide Area Network connections over leased lines, ISDN circuits, and frame relay permanent virtual circuits. The P1705 supports a single LAN and one or two WAN links (one ISDN BRI interface or two other WAN modules). The P1730 supports two independent LANs plus one WAN interface or a single LAN plus two WAN interface modules (if two ISDN BRI modules are installed, this will provide 4 WAN links)

PPP ISDN units provide bridging, IP/IPX routing, and compression over a PPP ISDN connection and support an ISDN BRI interface via an integral ISDN-ST or ISDN-U link module. The ISDN BRI interface supports two 64 Kbps B-channels.

PPP Lease line units provide bridging, IP/IPX routing, and compression and support one or two physical wide area network (WAN) links that may operate at speeds up to 2.048 Mbps.

Frame Relay units provide bridging and IP/IPX routing and support 1 to 128 Permanent Virtual Circuit (PVC) across two physical wide area links running RAW 1490 or encapsulated PPP.

The following instructions provide a quick set-up guide for installation of the P1705 & P1730 Ethernet Bridge/Routers:

Unpack the Router

Rough handling during shipment can damage electronic equipment. As you unpack the bridge/router, carefully check for signs of damage. If damage is suspected, contact the shipper. Save the box and all packing material to protect the bridge/router should it ever need to be moved or returned for service.

Check the packing slip that identifies the components and the LAN connector.

Select a Site

Place the bridge/router in a well ventilated area. The site should maintain normal office temperature and humidity levels. Air vents located on the sides of the bridge/router must have approximately one inch / 2.5 centimeters of clearance from any object.

Identify the Reset Switch

The small hole under the front right corner of the faceplate is used in case a hardware reset is required. The end of a paper clip is sufficient to toggle the small switch behind the hole.

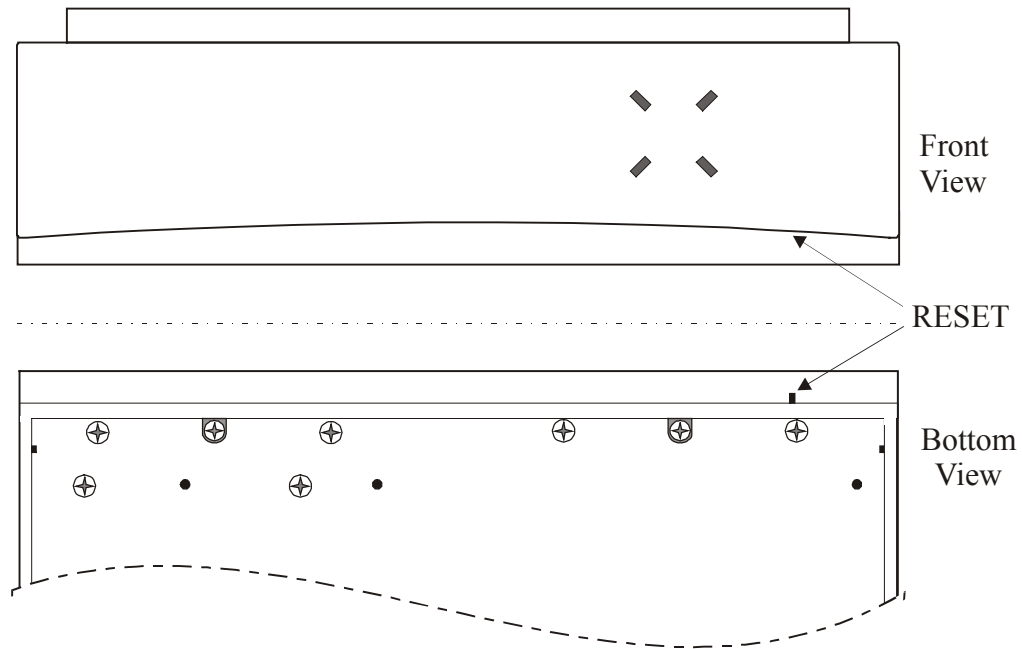


Figure 1-1 Location of the Reset Hole on Router

Identify the Connectors

P1705

The P1705 may be ordered with a 10Base2, 10Base5, or 10BaseT LAN interface.

If this P1705 has an ISDN U or S/T Module, it **must** only be installed in the slot 1 (leftmost position when viewed from the rear of the unit). The slot 2 position may be unused and covered with a blank panel or may contain another type of module. If a second WAN module is installed, only one BRI channel will be available for use.

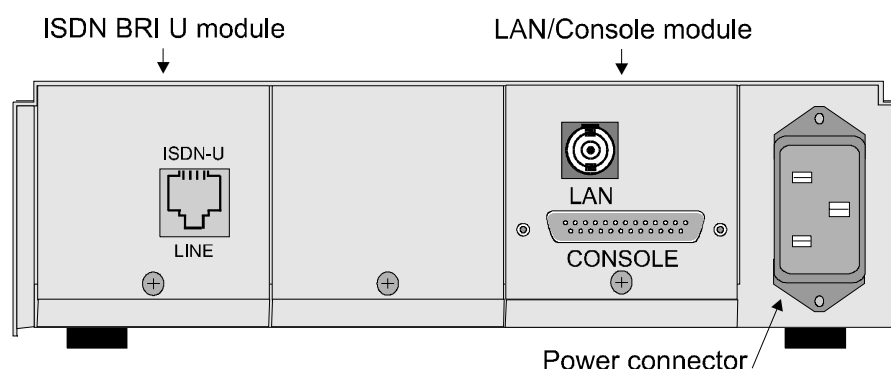


Figure 1-2 Rear View of the P1705 with ISDN interface

P1730

The P1730 is configured with a 10/100BaseT LAN and either one or two optional interface modules. The optional modules may be a second LAN (10 BaseT), a second LAN plus one WAN module, a single WAN module or two WAN modules.

Important: *If a second LAN module is installed, it must be in the slot 1 (leftmost position when viewed from the rear of the unit) to operate. In addition, if only one optional interface module is installed, it must be in slot 1*

Each interface may be changed by simply removing the existing module and installing a new module. Refer to Appendix D: Servicing Information for information on replacing modules.

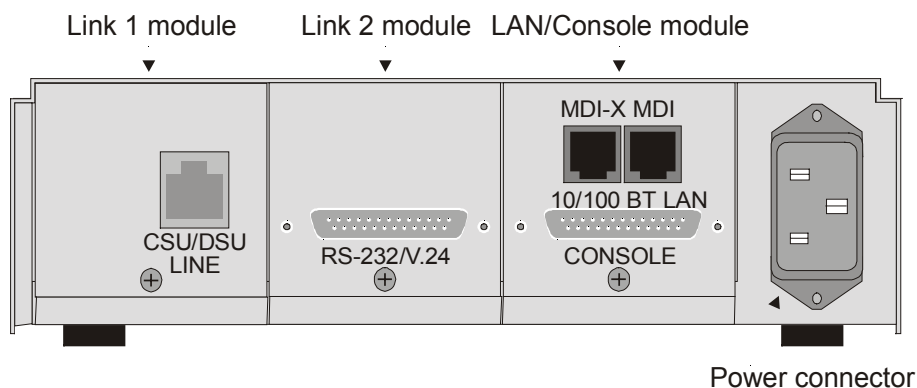


Figure 1 -3 Rear View of the P1730 with a single LAN connection and two WAN modules

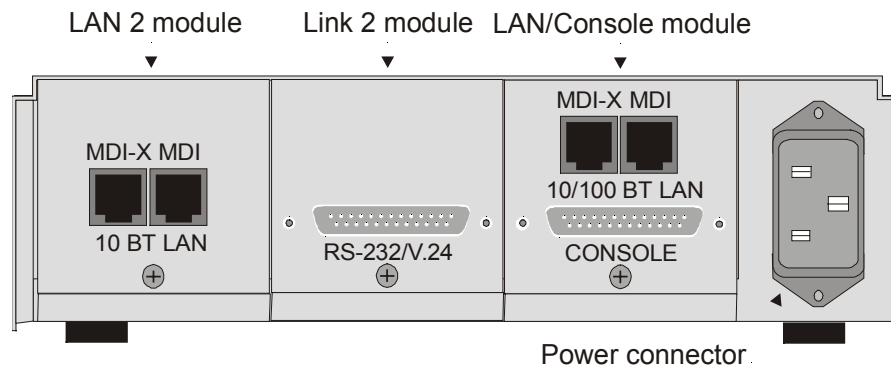


Figure 1-4 Rear View of the P1730 with Dual LAN connections and a single WAN module

Connect to the Console

Connection to the bridge/router operator's console is made through the DB25 connector labeled CONSOLE on the back of the bridge/router.

Connect the console port of the Router to a computer running an asynchronous communication package or a standard asynchronous terminal. The bridge/router supports autobaud rates at 1200, 2400, 9600, 19,200, 38,400 or 57,600 bps. Both the bridge/router and the bridged network are configured through the use of "hotkey" Menus.

Make the Link Connection(s)

By default the links are configured as permanent DTE interfaces. The clocking for each link will be provided by the DCE device connected to each link.

The V.35 link modules require interface converters that convert from a DB25 connector to a male 34-pin (V.35) connector used for the V.35 interface. Be sure to secure the cable connector(s) to the bridge/router and the communications equipment with the connector screws to prevent accidental disconnection.

The CSU/DSU module uses a RJ-48S connector to interface with the digital data service.

G.703 modules use a standard BNC connector with a 75 ohm cable.

The ISDN-ST interface module of the ISDN Router provides a RJ-45 connector to connect to the RJ-45 connector of the NT1 provided with your ISDN service.

The ISDN-U interface module of the ISDN Router provides an integrated NT1 with a RJ-45 connector to connect directly with your ISDN service.

Pinouts for the WAN connectors are listed in Appendix D of this manual.

Power Up the Bridge/Router

Once the LAN and Link connections are made and the console is connected to a terminal, you are ready to power-up the router. Connect the AC power cord to the back of the router and plug the cord into the AC wall outlet.

Observe the LEDs as the bridge/router powers up. The LEDs will go through a circular flashing pattern as the power-up diagnostics are performed. After the power-up diagnostics are finished, the Power LED will go from red to green.

Enter at least one <RETURN> (up to three if necessary) in order for the bridge/router to determine the baud rate of the terminal used for the console (i.e., autobaud). The following information will now be seen on the console connected to the bridge/router :

```
Terminals supported:
ansi, avt, ibm3101, qvt109, qvt102, qvt119, tvi925,
tvi950, vt52, vt100, wyse-50, wyse-vp, teletype
Enter terminal type:
```

Select the terminal type being used if listed and enter its name (in lower case) at the prompt, or choose the terminal type **teletype** if your terminal is not listed. This terminal type operates in scroll mode and may be used successfully until a custom terminal definition is created.

Managing the P1705 & P1730 Using the Menus

This section describes the minimum configuration parameters required when setting up the P1705 & P1730. Each of the configuration scenarios requires setting of operational parameters on the P1705 & P1730. The built-in menu system of the P1705 & P1730 is used to configure the unit.

The router menu system operates on a “hotkey” principle; navigating around the menu system is done by typing the number associated with the desired option; the P1705 & P1730 acts on the choice immediately (no need to hit the “enter” key).

The menu system consists of different menu levels each containing new configuration options. Navigation back out of a nested menu is easily accomplished by pressing the tab key. The tab key takes you to the previous menu level. If you wish to move from your current menu location directly to the main menu simply press the equals “=” key.

When choosing menu options that will toggle between values, simply pressing the number associated with that option will cause the options value to change. Each successive selection of the option will cause the option’s value to change again.

Some menu options require input from the operator. When selecting an option that requires a value, the menu system will display the range of values acceptable and a prompt symbol “>”. Enter the new value at the prompt symbol and press enter. Should you make an error in entering the new value, the <BACKSPACE> key (for most terminals) deletes the most recently entered characters.

Conventions

Throughout this section, P1705 & P1730 menu options are shown that are required for the various configuration choices. The appropriate menu options are shown in each instance in the following format:



Configuration Option Name

Location: Main

↳ Sub-Menu Name

↳ Sub-Menu Name

↳ *Option Name*

The configuration option is shown as well as the options location within the menu system. The ↳ character indicates that a sub-menu level must be chosen. The option name is finally shown in italics.

The keyboard graphic in the left margin indicates that this is information that the user will have to enter for configuration.



The note icon is used to provide miscellaneous information on the configuration and set-up of the router.

Configuration: *The Configuration Note is used to indicate that there may be a difference in configuration between the various operational modes of the router. This may mean for example that the remote site set-up is configured differently for an ISDN PPP router than for Frame Relay.*



The information icon is used to indicate that more information is available on this subject. The information is usually located within another document as specified.



The caution icon indicates that caution should be taken when performing this task.

Login to Bridge/Router and Enter the Required Configuration

At the login screen type a 1 and the default password to enter the menu system of the Router. The default password is “BRIDGE” (case sensitive) and should be changed if security is desired.

With the options of the built-in menu system, the router may be configured to operate within your environment.

Refer to the PPP Menus Manual file for your operating software on the accompanying CD-ROM for a complete description of all the Menu Options.

The menu system of the router may also be used to view system statistics.

Note: Bridge/Router database changes and statistics viewing may be done remotely by establishing Telnet connections to a partner bridge/router across the WAN. This is accomplished by selecting the “Telnet” option.



```

Location: Main
  ↘ Configuration
    ↘ Access Set-up
      ↘ Telnet Set-up
        ↘ Telnet
  
```

Specify the name or IP address of the router you wish to connect to for configuration purposes or viewing of statistics.

Noting the Device name at the top left of each Menu may identify the router being controlled.

If there is no data transmitted or received for a period of 5 minutes, the Telnet session will be disconnected.

To disconnect from the router being controlled, enter Control-C (^C).



Telnet security considerations: Telnet may be disabled to prevent remote access control of the router. If Telnet access is enabled, the device password should be changed to some value other than the default to prevent unauthorized access.



```

Location: Main
  ↘ Configuration
    ↘ Access Set-up
      ↘ Device Set-up
        ↘ Password
  
```

Mandatory Configuration

The P1705 & P1730 requires a minimum amount of mandatory configuration in order to operate. The following table identifies the configuration parameters that must be defined for proper operation under the operational states shown in the table.

Bridge	IP Router	IPX Router
none	IP Address	none

ISDN - U	ISDN – S/T	PPP ISDN
ISDN Switch Type	ISDN Switch Type	B channel assignment
Directory Numbers	Directory Numbers	Remote Site Profile

Frame Relay	Lease Line	PPP Lease Line
none (North America)	none	none (International)
		Remote Site Profile
Frame Relay enabled (International only)		Frame Relay disabled (North America only)

The configuration options required for proper initial operation are described in Section 2: Typical Applications and How to Configure Them. Each configuration requires a different set of parameters to be entered.

Refer to Section 2 for details on configuring the P1705 & P1730 in different operational states. Also refer to the P1705 & P1730 VPN Menus Manual file for your operating software on the accompanying CD-ROM for a complete description of all the Menu Options.

Other options may be changed depending upon specific installation configurations. Refer to the menu tree in Appendix A for a reference of the menu structure and options.

Setting the T1/E1 Parameters (T1/E1 WAN only)

The parameters required for a T1 or E1 connection may be obtained from your service provider. These may then be entered via the T1/E1 set-up menu to configure the router for that service.



T1/E1 Selection:

Location: Main
 ↳ Configuration
 ↳ Interfaces Set Up
 ↳ WAN Set Up
 ↳ Link Set Up
 ↳ T1/E1 Set Up
 ↳ Link mode
 T1 or E1

Set the service mode to which this router will be connected.



Service parameters:

Location: Main
 ↳ Configuration
 ↳ Interfaces Set Up
 ↳ WAN Set Up
 ↳ Link Set Up
 ↳ T1/E1 Set Up
 ↳ Speed/Channel rate
 56/64 kbps
 ↳ T1/E1 framing
 framed/unframed/SF/ESF
 ↳ Line encoding
 AMI/INV_AMI/
 B8ZS/HDB3

Select the service channel speed, framing format, and encoding as designated by the service provider.

T1 service requires the specification of a Line Build Out factor. This parameter modifies the transmitted signal to compensate for degradation due to line losses between the transmitter and receiver. A number of different options are available to meet standards for T1 long haul (direct connection to service providers central office facility), T1 short haul (connection through a local PBX), AT&T TR64211 specification long haul and AT&T TR64211 short haul. Your service provider will tell you which specification their service requires. Short haul LBOs are listed as the length of the cable run (in feet) between the router and the local exchange.

E1 service does not require line build out selection.



Set Link Interface Type:

Location: Main

- ↳ Configuration
 - ↳ Interfaces Set Up
 - ↳ WAN Set Up
 - ↳ Link Set Up
 - ↳ T1/E1 Set Up
 - ↳ LBO
 - as specified*

T1 long-haul LBOs: L0db, L7.5db, L15db, L22.5db

Short haul LBOs: S0to110ft, S110to220ft, S220to330ft, S330to440ft, S440to550ft, S550to660ft

AT&T standard TR64211 long-haul connection: TL0db

AT&T standard TR64211 short-haul connection: TS0to110ft, TS110to220ft, TS220to330ft, TS330to440ft, TS440to550ft, TS550to660ft

If fractional T1/E1 service is being provided, you will need to specify the channels/timeslots to be used.



Set Link Interface Type:

Location: Main

- ↳ Configuration
 - ↳ Interfaces Set Up
 - ↳ WAN Set Up
 - ↳ Link Set Up
 - ↳ T1/E1 Set Up
 - ↳ Slot/Channel Set Up
 - ↳ Start
 - first channel*
 - ↳ Number
 - number of channels*

Some E1 service providers reserve timeslot 16 for network management use. If your service specifies that timeslot 16 is for their use, toggle this option to *reserved*




Set Link Interface Type:


Location: Main


- ↳ Configuration
 - ↳ Interfaces Set Up
 - ↳ WAN Set Up
 - ↳ Link Set Up
 - ↳ T1/E1 Set Up
 - ↳ Slot/Channel Set Up
 - ↳ E1 Timeslot 16
 - reserved*


Identify the Status LEDs

The four three colour Light Emitting Diodes (LEDs) on the front of the router are depicted in Figure 1-1. The meanings of these LEDs are found in the following chart.

Off	Bridge/Router is powered down
Green	Bridge/Router is running and has passed power-up diagnostics
Green (flashing)	Bridge/Router is in BOOT mode and is programming the flash
Red	Bridge/Router is powered up but has failed power-up diagnostics
Yellow (flashing)	Bridge/Router is in BOOT mode
POWER 	

Off	Module is not installed
Green	Module is connected and forwarding
Yellow	LAN is connected and NOT forwarding: i.e. Listening, Learning, or Blocking
Red	Bridge/Router is NOT connected to the LAN
LAN 	

Off	Module is not installed or is configured to be down: Disabled.
Green	Connection is up* / LAN 2 connected and forwarding
Yellow	LINK is negotiating in ISDN. LINK is auto-learning LMI type in Frame Relay. Not used in Leased Line or LAN mode
Red	Software failure (if WAN module installed) LAN 2 not connected (if LAN2 module installed)
LINK 1/LAN 2 	

Off	Module is not installed or is configured to be down: Disabled.
Green	Connection is up*
Yellow	LINK is negotiating in ISDN. LINK is auto-learning LMI type in Frame Relay. Not used in Leased Line mode
Red	Software failure
LINK 2 	

*If the module is an ISDN BRI interface, a connection on either B-channel will display a green LED.

Typical Applications & How to Configure Them

The P1705 & P1730 are flexible Ethernet Bridge/Routers. This section will describe how to set-up the P1705 & P1730 routers using each of its networking functions. Note that depending on the model of unit and what interface modules are installed, some of the configuration examples may not apply; for example, if no ISDN BRI module is installed, the sections on setting up an ISDN PPP router would not apply.

The P1705 & P1730 routers may be configured as a simple Ethernet bridge, an Ethernet IP router, an Ethernet IPX router, or a combination of the three. When operating the router as a combination bridge/router, simply configure each of the components separately.

Note: *The configuration options described within this section are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P1705 & P1730 VPN Menus Manual file on the accompanying CD-ROM.*

Important: *The P1705 & P1730 uses FLASH memory to store the configuration information. Configuration settings are stored to FLASH memory after there has been 30 seconds of idle time. Idle time is when there is no selection or modification of the value in the built-in menu system. If you wish to save a configuration immediately, enter "=" to get to the main menu, then select option 5 "Save configuration".*

Bridging and Routing

Should You Bridge or Route?

When connecting two networks together, the first question to ask is “should I bridge or route”? The decision to bridge or to route may be decided by how the existing networks have been already set-up.

Bridging should be used when the network consists of non-routable protocols or routable protocols using the same network numbers. Some protocols can only be bridged; some of the more well known are NetBEUI (used by Microsoft Windows), and LAT (used by Digital Equipment Corp.).

If your IPX or IP network address is the same at both locations, bridging is simpler and requires less configuration. If the locations are to be routed together, the network numbers will have to be different in both cases; this could require extensive reconfiguration.

IPX routing should be used if the two locations are already set-up with different IPX network numbers. Routing IPX will minimize the number of SAP and RIP messages being sent across the WAN.

IP routing should be used if the two locations are already set-up with different IP network numbers or if you wish to divide your one IP network number into two sub-networks.

In some cases both bridging and routing may be required. Routing may be required for IP information and bridging may be required for NetBEUI.

Bridging

An Ethernet bridge intelligently forwards Ethernet data packet traffic between connected networks. The traffic may be across the Wide Area Network (illustrated below) or, in the case of the P1730, may be between two LANs connected to the same P1730.

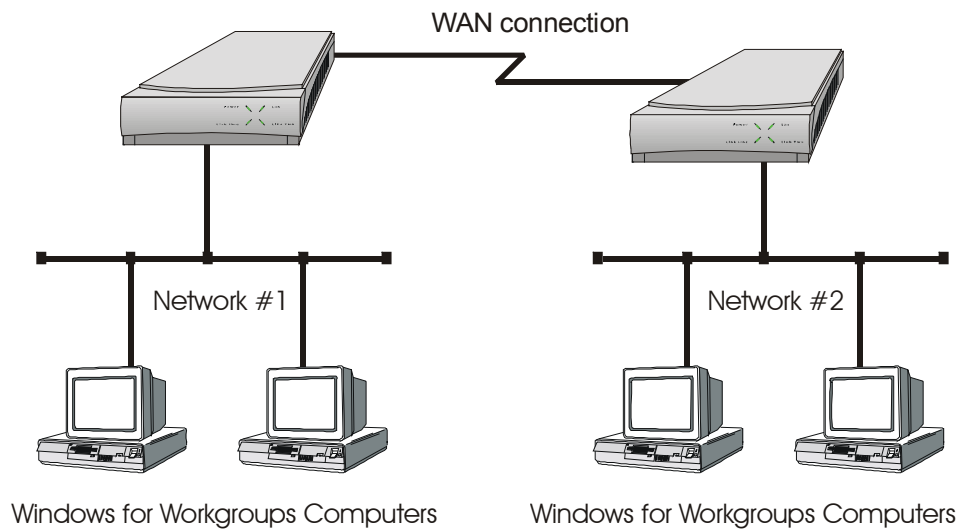


Figure 2 -1 Networks Bridged across a WAN link

Ethernet bridges simply forward information based on Ethernet MAC addresses. If a packet is destined for a device located on a different network than the device that sent the packet, the bridge will forward that packet to the connected network. If a packet is destined for a device located on the same local network as the originating device, the bridge will ignore the packet.

Ethernet bridges also communicate to each other using what is called the Spanning Tree Protocol (STP). STP is used to prevent loops in a network which cause traffic to be re-broadcast again and again causing network congestion.

The P1705 & P1730 are pre-configured to operate as an Ethernet bridge compatible with the IEEE 802.1d Spanning Tree Protocol definitions. This means that without configuration modifications, the P1705 & P1730 will bridge Ethernet traffic to its partner bridges when the Wide Area Network (WAN) connection has been established.

The P1705 & P1730 are also pre-configured as an IPX router. This means that if you wish to bridge IPX traffic instead of routing it, you must disable the IPX routing function of the router. Once IPX routing has been disabled, all IPX traffic will be bridged between networks.

To set-up a bridge between two LANs using a dual LAN P1730, all that is required is that the LANs be connected to the router.

To set-up a bridge between two networks connected by a WAN link:

- Connect each router to the LAN(s) it will be serving
- Connect the WAN interface of each router to the equipment supplied by the service provider
- Configure the remote site profile of the partner router if necessary
- Establish the WAN connection

IP Routing

An Ethernet IP router is used to intelligently route Internet Protocol (IP) traffic to another network. The networks may be connected across a WAN link (illustrated below) or two LANs connected to the same dual LAN P1730.

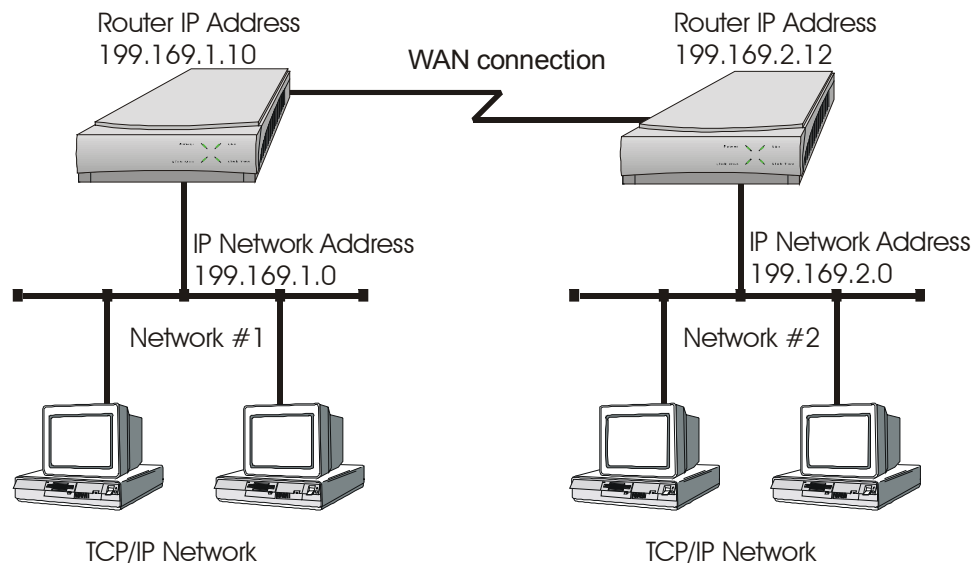


Figure 2 -2 IP Networks Routed across a WAN link

IP routers forward IP frames based upon their IP destination address and an internal routing table. The router maintains the internal routing table with the connected network IP addresses and, for WAN link connections, the remote partner IP routers associated with those networks. When an IP frame is received, the destination IP address is examined and looked up in the routing table. In the case of a dual LAN router, if the destination IP address is on the other LAN, the packet is routed there. For WAN connections, if the destination IP network is found in the routing tables, the IP router sends the IP frame to the remote partner router that is connected to the appropriate remote IP network. If no explicit route entry is found in the routing table, the IP frame is sent to the Default Gateway. The Default Gateway may be learned from the LAN or may be set manually (see section 2.1.2.3).

To configure an router for IP routing between networks, the following parameters must be defined in the built-in menu system.



1. IP Address

Location: Main

- ↳ Configuration
- ↳ Interfaces Set-up
- ↳ LAN Set-up
- ↳ IP Set-up
- ↳ *IP Address / Size of Subnet Mask*

If this P1730 has the dual LAN option installed, you will first be asked which LAN to reference (1 or 2). Both LANs must have unique IP addresses to use IP routing.

IP Addressing

Devices on an IP network are located by their IP addresses, which is a 32 bit number divided into four 8 bit fields. The IP address identifies both the network and the host device (also known as a node) on that network. The address is usually written as the four decimal values for the fields (between 0 and 255) separated by decimal points; for example 196.65.43.21.

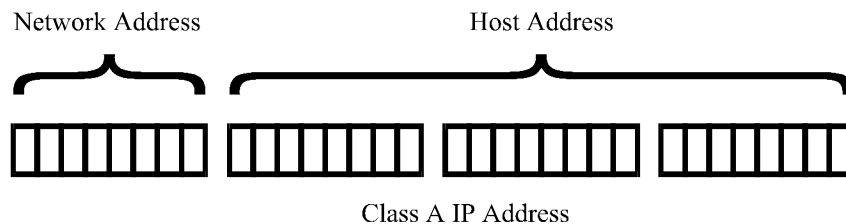
The high order field defines the IP class of the address. There are three commonly used classes of standard IP addresses:

A: 1 to 127

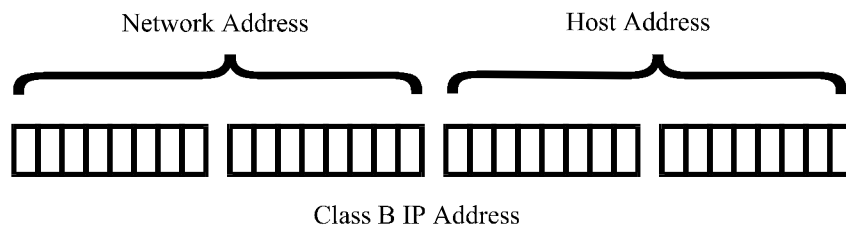
B: 128 to 191

C: 192 to 223

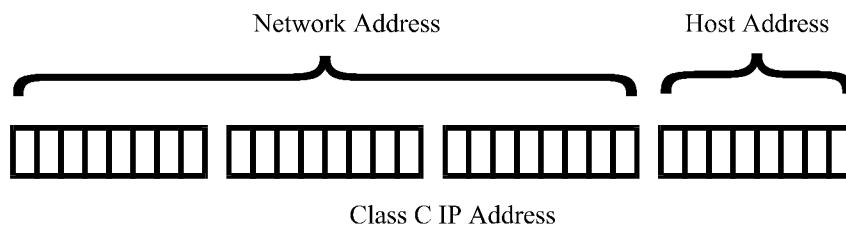
For Class A addresses, only the first 7 bits of the high order field represents the network address, so there can be 127 networks. The remaining three fields are the host portion of the address – there can be over 16 million (2^{24}) host devices on each class A network.



Class B uses the first two fields for network addresses and can address approximately 16,000 networks. The two low order fields allow approximately 65,000 host addresses (2^{16}) for each network.

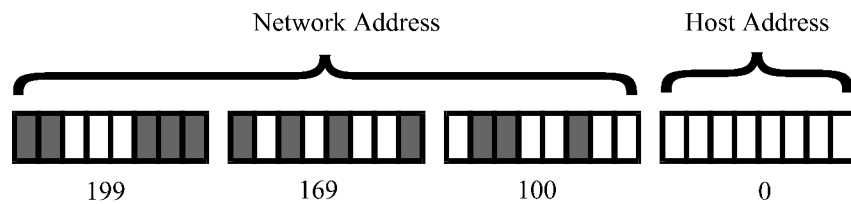


Class C uses three high order fields to address over 2 million networks; the low order field is used to address up to 253 hosts (the addresses with all bits set to 1 and all 0 are reserved for network use; so addresses available from 8 bits = 255 minus the 2 reserved).



IP addresses within a private network may be assigned arbitrarily, however, if that network is to interconnect with the global Internet, it is necessary to obtain a registered IP address.

For example, a small company is connected to the Internet; they are assigned a single class C IP network address (199.169.100.0). This network address allows the company to define up to 253 host addresses within their network.



Masks

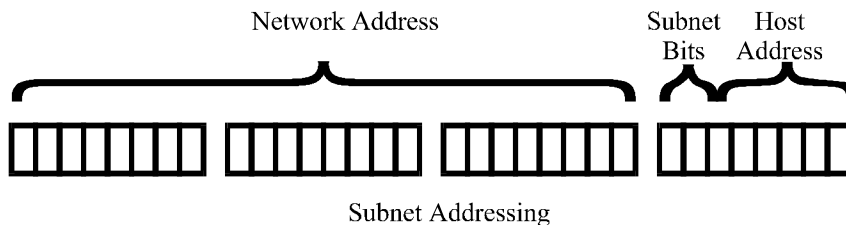
The portion of the IP address to use as the network address is specified by using a mask; a mask is the contiguous number of bits to be used for the network address all set to 1. When the mask is logically ANDed with an IP address, the result is the network address. The mask is specified by entering the mask size as the number of bits in the mask. For the standard Class A, B and C Internet addresses, the mask sizes would be 8, 16 and 24 respectively.

Networks are not restricted to the above standard sizes; the mask (and hence the network address it specifies) may be any number of bits from 8 to 32. This gives much more flexibility to match the size of the two fields of the IP address to the number of networks and hosts to be serviced.

IP Subnets

An IP network may be divided into smaller networks by a process called sub-netting. A subnet is specified using some of the high order bits of the host field of the IP address for sub-network addressing. The portion of the IP address to be used as the subnet address is defined by using a subnet mask.

If the company in the example above (Class C IP address 199.169.100.0) decides to split their network into two LANs to reduce the load on their network, the original IP network address may be sub-netted into two or more smaller IP networks consisting of a smaller number of host addresses in each LAN. This allows each of the sites to be a smaller IP network and to be routed together to allow inter-network communication.



The subnet mask size is the number of bits in the subnet mask. In the above figure the subnet mask size would be 26 (24 bits for the class C network address and 2 subnet bits). The subnet size is the number of subnet bits - in the above figure, the subnet size would be 2.

Typical Applications & How to Configure Them

The P1705 & P1730 allows mask sizes from 8 to 32 bits. The subnet mask size determines how many bits of the host field of the original IP network address will be used for the creation of subnets. In this example, specifying a mask size of 26 will produce a subnet size of 2 bits. Two bits gives 4 possible sub-network addresses from the original IP network address. Two of the resulting sub-networks will have either all zeros or all ones as the subnet address; these addresses are reserved for network functions and hence are invalid addresses. The subnet mask for the above example networks will be 255.255.255.192:



So setting a subnet mask size of 26 will generate two sub-networks with up to 62 host addresses each (64 potential addresses minus the all zero and all one addresses). The new IP sub-network addresses will be: 199.169.100.64 and 199.169.100.128.

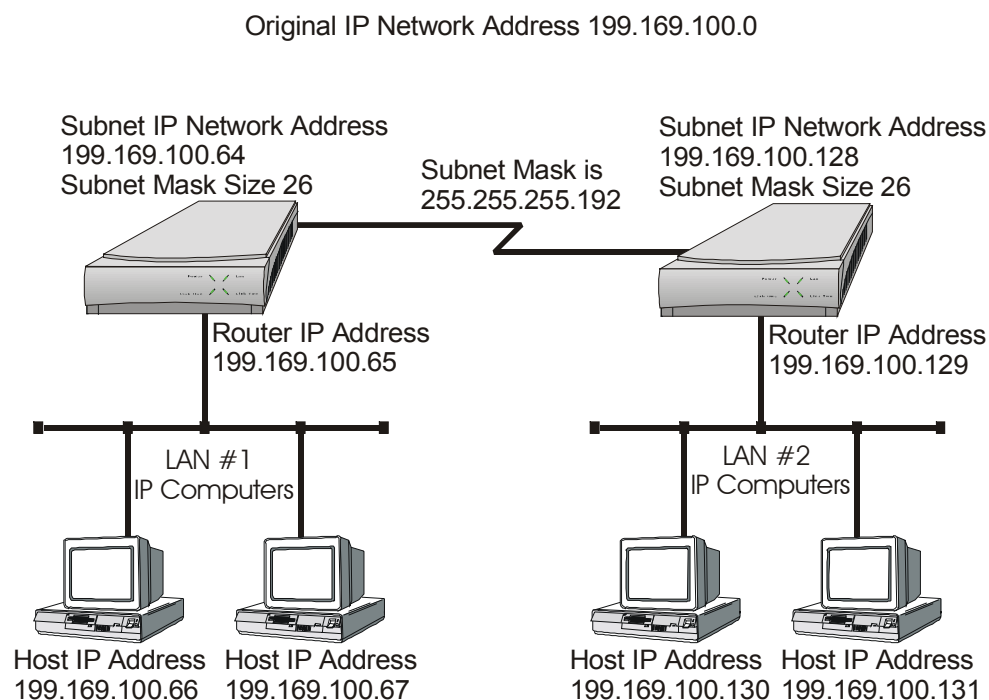


Figure 2 -2 Defining an IP Subnet Mask

IP Default Gateway

An IP default gateway is an IP router that is resident on the local IP network that this router is connected to and is used to route IP frames for destination networks that do not exist in the routing table. When an IP frame is received that is destined for a network that is not listed in the routing table of the router, the router will send the IP frame to the default gateway. If the device originating the IP frame is on the same LAN as the router, the router will then send an ICMP redirect message to the originating device. Any future IP frames for that destination network will then be sent directly to the default gateway instead of the router.

A default gateway may be configured if there are a large number of routes that will pass through another router to a larger network. An example of this would be a router that is used to connect to the Internet. All of the routers on the LAN would have the Internet access router as the default gateway.

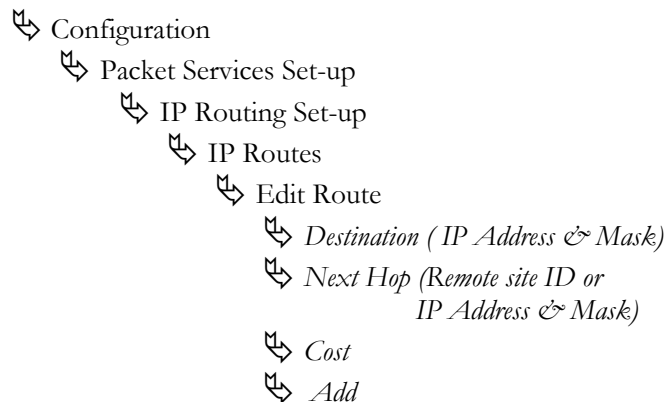
IP Static Route

With its default settings, the P1705 & P1730 will automatically learn the routes to other devices on the network through RIP messages. In some instances it may be desirable to have a predetermined or static route that will always be used to reach certain devices, such as when one specific router is to be used to reach a destination IP network. The static route will have precedence over all learned RIP routes even if the cost of the RIP learned routes is lower.



Edit Static Route

Location: Main



Each static IP route is defined in the Edit Route menu. The destination network IP address is specified when you first enter the menu and then the IP address, alias or ID number of the next hop route and the cost may be defined. Finally, select *Add* to add the route to the routing table.

Once static IP routes are defined, they may be viewed with the *Show Static Routes* command from the IP Routes menu.

Configuration: When the IP routing protocol is set to none, static routes will be used to route traffic. The mask size must also be defined when creating a static route entry. The subnet mask is required to allow a static route to be created to a different IP network address. See the previous section for an explanation of masks.

IPX Routing

The P1705 & P1730 are pre-configured to operate as an IPX router. When installed in an IPX network, the router will learn the IPX network numbers from connected networks. It will then route the IPX frames to the appropriate destination IPX network.

The IPX routing scenario may consist of one of the two following configurations. The first configuration consists of Novell servers located on each of the LAN segments to be connected. The second configuration consists of Novell servers located on only one of the LAN segments to be connected. The router IPX router will need to be configured differently in the second configuration with Novell servers located on only one of the LAN segments.

Novell Servers in Both Locations

An Ethernet IPX router is used to intelligently route Novell IPX LAN traffic to another network. The networks may be connected across a WAN link (illustrated below) or two LANs connected to a dual LAN P1730.

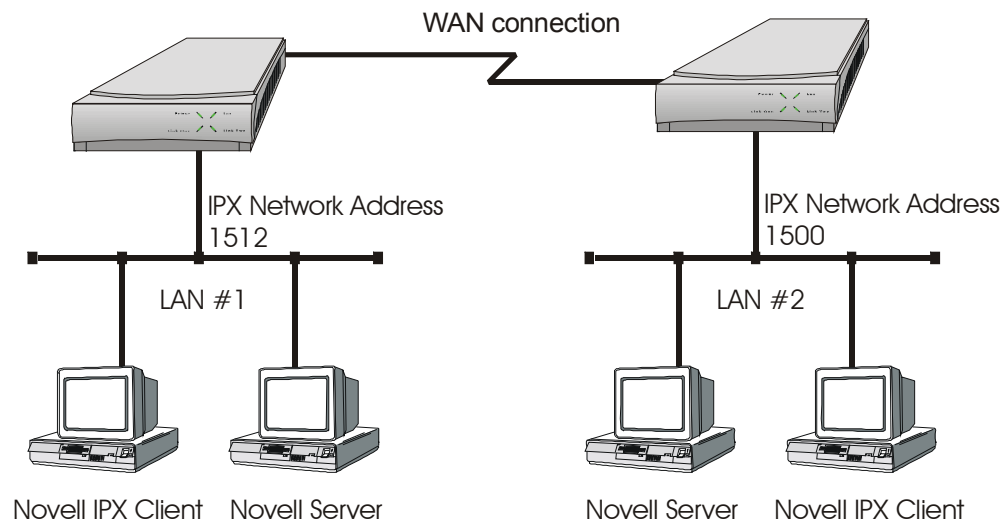


Figure 2 -3 IPX Routed Local Area Networks (Servers on both sides)

IPX routers forward IPX frames based upon their IPX destination address and an internal routing table. The router maintains the internal routing table with the network IPX addresses and the remote partner IPX routers associated with those networks. When an IPX frame is received, the destination IPX address is examined and looked up in the routing tables. Once the destination IPX address is found in the routing tables, the IPX router sends the IPX frame to the appropriate remote IPX network.

When both LAN segments contain Novell servers, the IPX network numbers are learned automatically; simply ensure that IPX routing is enabled on the router for both networks.

*When two IPX LAN segments with Novell servers on each segment are to be connected via IPX routing, you must ensure that the IPX network numbers on each of the Novell servers is **unique**. If the IPX network numbers are the same, IPX routing will not operate.*

Once the WAN connections have been established to the remote partner routers, the IPX router portion of the routers will begin to build their routing tables according

to the IPX frames they receive from the network. Manual entries may be made in the routing tables by adding static IPX routes.

Novell Servers in One Location Only

Some Novell LAN installations require that a remote LAN that consists of only Novell IPX clients be connected to a central LAN that contains the Novell servers and some more clients. In this configuration, the router IPX router located at the remote site must be configured with the appropriate IPX network numbers. The IPX network number must be configured manually because there is no Novell server at the remote site. The router must act as a Novell server to supply the proper IPX network number to the clients on the remote site LAN.

In the following diagram, the router connected to LAN #2 must be configured with IPX network number 1500 (or any other valid, unique IPX network number) using the appropriate frame type. The clients connected to LAN #2 must also be running with the same frame type as defined on the router. After the routers have established the WAN connection, the IPX routing procedures will cause the names of the services located on LAN #1 to be stored in the services table on the router on LAN #2. When one of the clients on LAN #2 starts up, it will look for a server on the local LAN and the router will respond with the list of servers that are located on LAN #1.

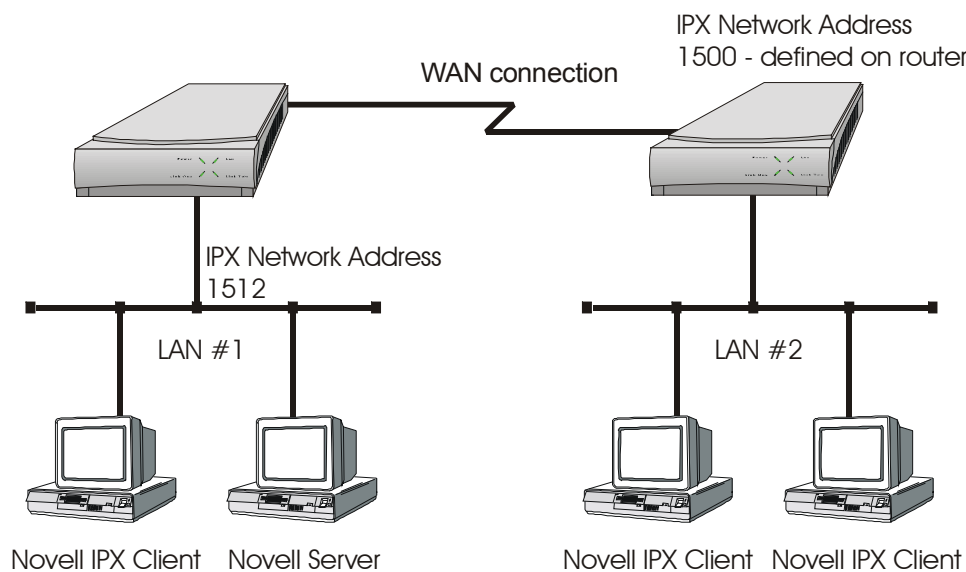


Figure 2 -4 IPX Routed Local Area Networks (Servers on one side)

The following steps must be performed on the router connected to LAN #2.



IPX Routing Disabled

Location: Main

- ↳ Configuration
- ↳ Packet Services Set-up
- ↳ IPX Routing Set-up
- ↳ *IPX Routing*

Disabling IPX routing allows the IPX frame types to be modified.

Configuration: *IPX Routing does not need to be disabled in order to change the defined network numbers on a PPP router.*

Note

IPX Frame Types



Location: Main

- ↳ Configuration
- ↳ Interfaces Set-up
- ↳ LAN Set-up
- ↳ LAN IPX Set-up
 - ↳ *Ethernet-II Frames*
 - ↳ *RAW 802.3 Frames*
 - ↳ *IEEE 802.2 Frames*
 - ↳ *802.2 SNAP Frames*

Define the IPX network number for the appropriate frame type. Note that IPX network numbers must be unique. If more than one frame type is to be used, each frame type must have a unique IPX network number. There must be no duplicate IPX network numbers within your entire IPX routed network they must all be unique. The IPX network numbers may be any value from 0 to FFFFFFFF HEX.



IPX Routing Enabled

Location: Main

- ↳ Configuration
- ↳ Packet Services Set-up
- ↳ IPX Routing Set-up
- ↳ *IPX Routing*

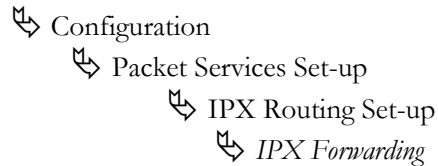
IPX routing must be re-enabled to allow the router to operate as an IPX router with the newly defined IPX network numbers.

All connected router IPX routers must have IPX routing enabled for IPX routing to take place between the LANs. When one of the routers on a network has IPX routing disabled, all of the router IPX routers will become bridges only for IPX frames.



IPX Forwarding Enabled

Location: Main



IPX forwarding must be re-enabled to allow the router to forward IPX frames onto the WAN to the partner router IPX routers.

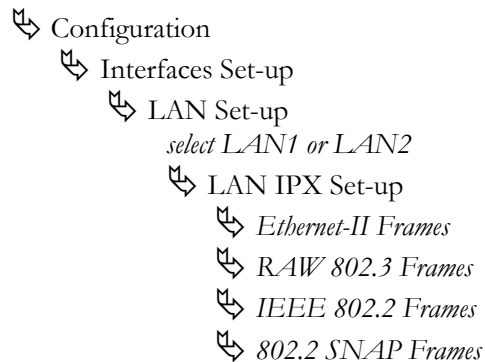
The IPX Forwarding function enables or disables the forwarding of IPX traffic when IPX routing is enabled. When IPX forwarding is disabled, all IPX traffic across the WAN links will be blocked. While IPX forwarding is disabled, the router will still operate as an IPX router and maintain its routing and server tables.

Novell Server with Dual LANs

If an P1730 is configured with two LAN interface modules, the setup will be similar to the above configuration; the difference being that rather than configuring the IPX numbers on different routers, they are configured on different LANs.

IPX Frame Types

Location: Main



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P1705 & P1730 VPN Menus Manual file on the accompanying CD-ROM.

PPP Overview

Point to Point Protocol (PPP) is a connection protocol that allows control over the set-up and monitoring of network communications. It is used in procedures for user authentication (name and password), connection management (spoofing, bandwidth on demand, multilink), and compression. If any these functions are required on a frame relay connection, PPP encapsulation within frame relay is available.

PPP Link Configuration

A PPP connection between two routers may use a number of Network Control Protocols for communication. An IP router connection will use the Internet Protocol Control Protocol (IPCP) for all IP communications. An IPX router connection will use the Internet Packet Exchange Control Protocol (IPXCP) for all IPX communications.

In order to establish an IPCP or IPXCP link connection between two PPP routers, either a numbered link or an unnumbered link connection must be established. The two types of link connections are available to allow for greater flexibility between vendors products.

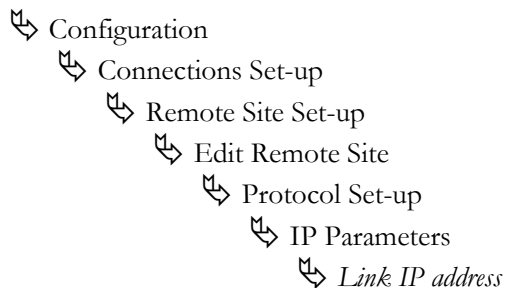
Numbered Links

A numbered link assigns a network address (either IP or IPX) to both ends of the WAN connection. In a numbered link configuration, the WAN connection may be viewed as another LAN network with the two PPP routers simply routing information between their local LANs and the common connected WAN network.

Because the WAN is considered a separate network, each of the stations on that network must be assigned a network address. If a numbered IP link is to be established, then each WAN interface must be assigned an IP address on a unique IP network. The WAN IP network address must be different from the two existing networks that are being connected together with the PPP routers.



Location: Main



If a numbered IPX link is to be established, then each WAN interface must be assigned an IPX node address on a unique IPX network number. The WAN IPX network address must be different from the two existing networks that are being connected together with the PPP routers.

The IPX node address of the local WAN link is defined as the **Local IPX Node** within the remote site profile settings. The IPX address of the WAN link of the remote PPP router is defined as the **Peer IPX Node** within the remote site profile settings. The WAN IPX network number is defined with the **IPX Net** option in the remote site profile settings.

Unnumbered Links

An unnumbered link does not use network addressing on the WAN link. The WAN connection is roughly equivalent to an internal connection with each of the two end point routers operating as half of a complete router that is connected between the two endpoint LANs.

When an IPCP link is set to unnumbered, the only configuration option applicable is **Peer IP Address**. The peer IP address in this case is the IP address of the remote PPP router, that is the IP address of its LAN connection. If the peer IP address is not specified, the router will attempt to determine it when negotiating the IPCP connection.

When an IPXCP link is set to unnumbered, no addressing configuration is required. All of the IPX settings are negotiated during the IPXCP connection.



When making a raw frame relay (no PPP encapsulation) connection with unnumbered links, the IP network address of each partner router must be manually entered in the remote site set-up for the link to operate.



Location: Main

- ↳ Configuration
- ↳ Connections Set-up
- ↳ Remote Site Set-up
- ↳ Edit Remote Site
- ↳ Protocol Set-up
- ↳ IP Parameters
- ↳ Peer IP address

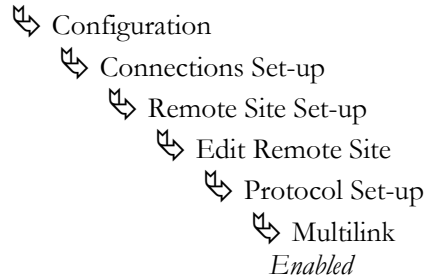
Multilink Operation

Multilink operation defines the use of more than one link to connect between two PPP routers. The **MultiLink Operation** option of the remote site profile for a connection is enabled by default.

When a Multilink connection is established, the Multilink (MP) options within the PPP set-up and Advanced PPP set-up menus will determine the operation of the Multilink connection.



Location: Main



Basic WAN Configurations

Basic ISDN Connections

If this P1705 & P1730 are configured as an ISDN bridge/router, it may establish WAN connections to other bridge/routers via ISDN (Integrated Services Digital Network) connections.

Before the P1705 & P1730 can establish an ISDN connection to another ISDN router, the ISDN information must be defined. The ISDN switch type must be defined for the ISDN interface, and the phone numbers must be defined. Refer to the following diagram that shows three router units connected together with two ISDN B-channels being configured on each unit.

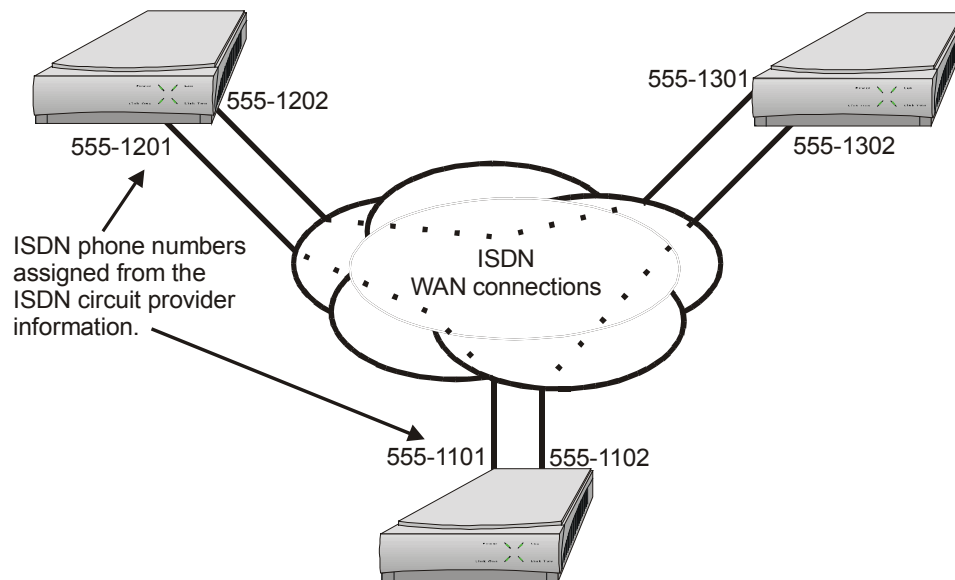


Figure 2 -5 Basic ISDN Configuration

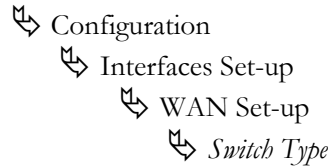
The following steps must be performed to configure the P1705 & P1730:

The default switch type for ISDN S/T interface modules is NET3, the default switch type for ISDN U interface modules is NI-1. If the type of service your provider uses matches the default setting for the interface module, the following step may be skipped, otherwise, the switch type must be set.



Switch Type

Location: Main

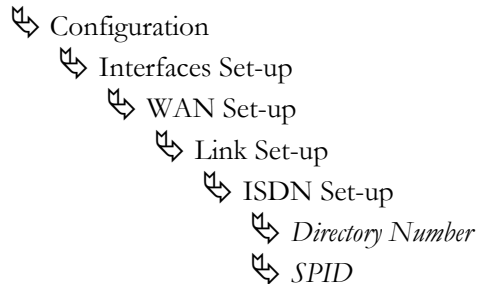


Ten ISDN switch types are available: net3, ni-1, ni-2, dms-100, 5ess-pp, 5ess-mp, tph1962, kdd, sweden, or ntt. Note that if your routers are located within different ISDN jurisdictions, the ISDN switch type may be different on each of the units.



Directory Numbers & SPIDs

Location: Main



The directory number will be the ISDN phone number used to establish a call between the routers. The SPID is used to register the ISDN interface with the central switch.



For switch type NET3, only one directory number is required. The router will operate without putting in the directory number for a NET3 switch, but it is recommended that it be entered.

Most North American installations use the switch type NI-1 and must have the directory number entered, as well the SPID (Service Profile Identifiers) value. For an NI-1 switch type, enter only the local portion of the directory number unless the area code is required for local calls. The SPID must be set to the exact number given by the ISDN service provider.

Once the ISDN switch type and directory numbers have been configured, the router must be reset for the new values to take effect and for the ISDN BRI interface to register with the central switch.



Soft Reset

Location: Main

↳ Diagnostics

↳ *Soft Reset*

Once the router has restarted it is ready to establish ISDN connections.

With the ISDN numbers and switch type defined, an ISDN call may be placed to another properly configured bridge/router. The calls may be placed manually or automatically. The automatic call features available are Auto-Call or IP Address Connect. An Auto-Call connection is established each time the router starts up. An IP Address Connect call is established to a specifically configured remote router when certain IP traffic is received from the local LAN.

Note that any time the switch type is changed a soft reset must be performed before the change will take effect.



The switch type is not saved through a full reset; the router will come up with the default switch type – NET3; if you require a different switch type, it must be re-entered after a configuration reload. It is strongly recommended that the entire configuration set of the router be saved (Dump config.txt to the console) then reloaded (Restore config.txt from the console) after a full reset.



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available, please refer to the “P1705 & P1730 VPN Menus Reference Manual.PDF” on the accompanying CD-ROM.

PPP ISDN Manual Call Quick Connections

The PPP P1705 & P1730 **should be configured** with a **remote site profile** entry for each router that will be called (see section 2.3.1). A manual direct dial connection may be performed to establish an initial connection to a remote site router. Once the connection is established and working properly, the remote site configuration for that router should be entered into the router. The remote site profile enables ISDN calls to be placed automatically each time the router starts up (Auto-Call) or automatically depending upon the time of day activation schedule or upon receiving IP frames from the local LAN destined for the IP network connected to that particular PPP router.

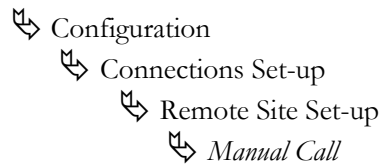
IPX Router Manual Call Connection

To establish an IPX PPP direct dial connection, enter the ISDN phone number of the remote site PPP router in the manual dial option. Refer to the Configure as an Ethernet IPX Router section 2.3.1 for more information on IPX configuration required.



Manual Call

Location: Main



Enter the ISDN phone number of the remote site IPX PPP router and an ISDN call will be placed.

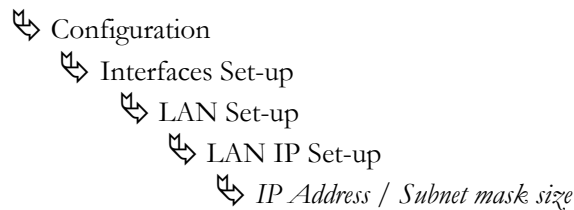
IP Router Manual Call Connection

To establish an IP PPP direct dial connection, the IP addresses must be supplied for this device before the ISDN call may be placed. Refer to the Configure as an Ethernet IP Router section 2.1.2 for more information on the IP configuration required.



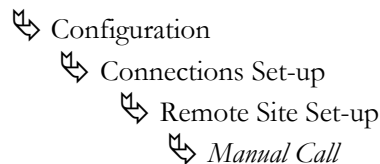
IP Address

Location: Main



Manual Call

Location: Main



Enter the ISDN phone number of the remote site IP PPP router and an ISDN call will be placed.

Basic Frame Relay Configuration

North American P1705 & P1730 with at least one non-ISDN interface are configured to have frame relay enabled for that interface by default. P1705 & P1730 shipped outside of North America with at least one non-ISDN interface will have frame relay disabled on that interface as a default setting. See the following page for instructions on switching Frame relay from disabled to enabled.

If the P1730 or P1705 is configured as a frame relay router, it will communicate over WAN connections to other Frame Relay units via Frame Relay Permanent Virtual Circuits (PVC). From 1 to 128 PVC's may be defined to connect to other frame relay units. Before the P1730 or P1705 can establish a PVC connection to another frame relay router, at least one PVC must be defined. The router is pre-configured to query the frame relay service to auto-learn the required parameters; they may also be set manually.

The DLCI (Data Link Connection Identifier) number for the PVC is assigned by the frame relay service provider. The PVC must be defined on at least one physical links on the router. Refer to the following diagram that shows three router units connected together with two PVCs being configured on each unit. The configuration of the PVCs within the frame relay cloud is controlled by the frame relay service provider.

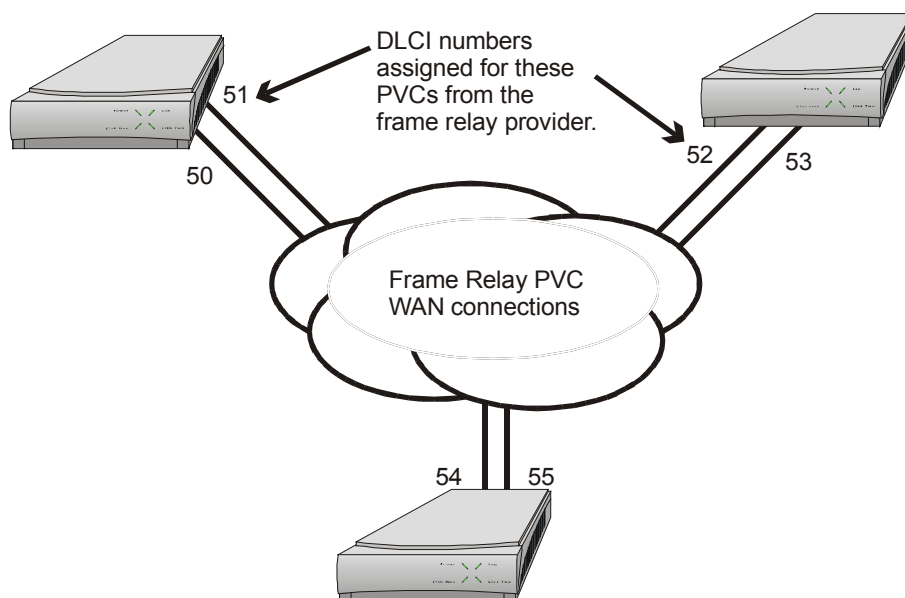


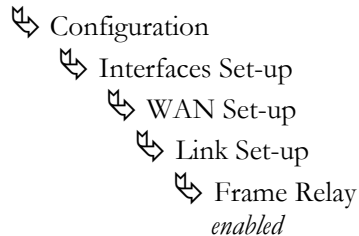
Figure 2 -8 Frame Relay configuration

Configuration: *The default configuration for P1705 & P1730 shipped outside North America is to have frame relay disabled. To run frame relay on these routers, it must first be enabled. Selecting the Frame Relay option will toggle the setting from disabled to enabled.*



Frame Relay enable

Location: Main



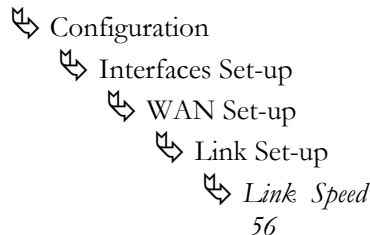
The router will request confirmation of the change, enter “yes”.

For an P1705 & P1730 with a CSU-DSU interface, the default clock speed that the P1705 & P1730 will expect to receive from the DCE link is 64Kbps. If the DCE link is 56 Kbps, then the Link Speed value must be reset to 56 here.



Link Speed

Location: Main



Auto Learning the Frame Relay Configuration

The P1705 & P1730 are pre-configured to query the frame relay service to auto-learn the LMI type and the PVC DLCI numbers. This auto-learn function allows the P1705 & P1730 to be plugged into the frame relay service and auto-learn the PVC configuration to become operational without further manual configuration. Router auto-learning conforms to RFC1490.

Manual configuration is also allowed by modifying the options within each Remote Site Profile and the individual link configuration menus.

When the P1730 or P1705 first starts up it will query the frame relay service to try to determine the LMI type on each of the frame relay links. Once the LMI type is determined, the PVC configurations will be known from the full status enquiry messages. If the DLCI numbers of the PVC's on your service are determined during this learning

process, the router will automatically create a remote site profile for each PVC. The automatically created remote site profiles will be named “LinkxDLCIyyy” where x is the physical link number the PVC is on and yyy is the DLCI of the PVC.



If during this learning process the maximum number of remote sites has been reached, the router will prompt you that there are no remote sites available. A new remote site cannot be auto-created unless one of the existing remote sites is manually deleted.



Auto-learning with PPP encapsulation enabled (see following page) may not be compatible with some older model routers. If problems with auto-learning occur with PPP enabled, try disabling PPP encapsulation.

Manual Configuration - LMI Type

The LMI Type option allows you to manually specify the type of Link Management Interface in use by the Frame Relay service provider for the Frame Relay service.

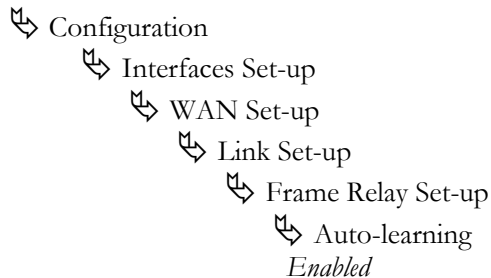
When the LMI type is set to none, the router simply creates frame relay packets and sends them on the defined PVC's. The links are not checked for errors. There is no congestion control checking. The link is only monitored for control signals.

To manually configure the LMI type the Auto-Learning option must be disabled.



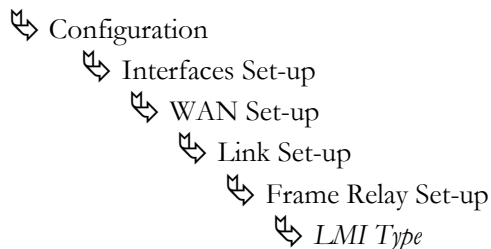
Auto-Learning

Location: Main



LMI Type

Location: Main



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the “P1705 & P1730 VPN Menus Reference Manual” file on the accompanying CD-ROM.

Quick Start Frame Relay

Since the P1705 & P1730 auto-learn the frame relay configuration, only a couple of parameters need to be configured before the unit is fully operational as an IP router for frame relay.

Upon initial start up, the P1705 & P1730 are pre-configured to query the frame relay service to auto-learn the LMI type and the PVC DLCI numbers. The P1705 & P1730 will then automatically create a remote site profile for each PVC.

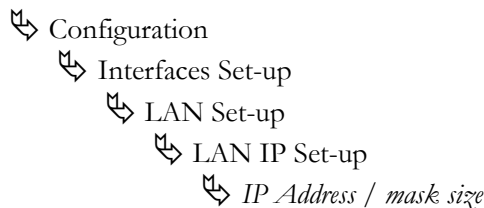
Within each of the remote site profiles automatically created Bridging, IP routing, and IPX routing are all set to “enabled”. Because each of these options are enabled by default and the automatically created remote site profiles will establish a PVC connection to the remote site routers, the P1705 & P1730 will bridge and IPX route data without any user configuration. Because an IP router requires an IP address, the router must be configured with an IP address before IP routing is fully operational.

To configure an IP address for the P1705 & P1730, use the IP address option.



IP Address

Location: Main



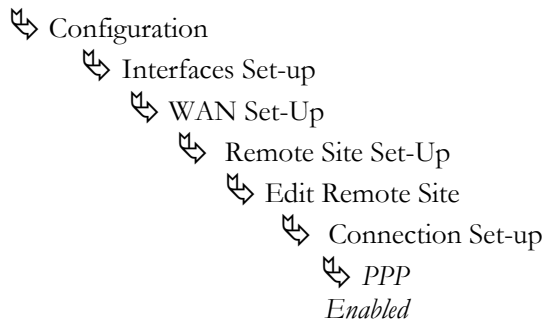
If security is required for the PVC connection refer to the Configure PPP Security section for information on setting the security passwords and user names for PPP.

By default, PPP is disabled for each of the newly created remote site profiles. If PPP encapsulation is desired, for example to use security, the PPP encapsulation option should be set to “enabled”. By default, when PPP encapsulation is enabled multilink is also enabled.



PPP Encapsulation

Location: Main



Basic Leased Line Configuration

The P1705 & P1730 establishes PPP (Point to Point Protocol) WAN connections to other PPP Leased Line routers or to other vendors PPP leased line routers via direct leased line connections. Either 1 or 2 links may be used to connect to other PPP routers.

Configuration: The default configuration for P1705 & P1730 shipped within North American with at least one non-ISDN interface module, is to have frame relay enabled on that interface. To run PPP leased line, frame relay must be disabled. Selecting the Frame Relay option will toggle the setting from enabled to disabled.



Frame Relay disable

Location: Main
 ↳ Configuration
 ↳ Interfaces Set-up
 ↳ WAN Set-up
 ↳ Link Set-up
 ↳ Frame Relay
 disabled

The router will request confirmation of the change, enter “yes”.

Quick Start PPP Leased Line Connections

A Quick Start minimal configuration may be used to initially establish a connection to another vendors PPP router. Once the connection is established and is working properly, the router **should be configured** with a **remote site profile** entry for that vendors router.

Before the P1705 & P1730 can establish a link connection to another PPP router, the link speed information must be defined. Refer to the following diagram that shows two routers and another vendors unit connected together with direct leased line connections.

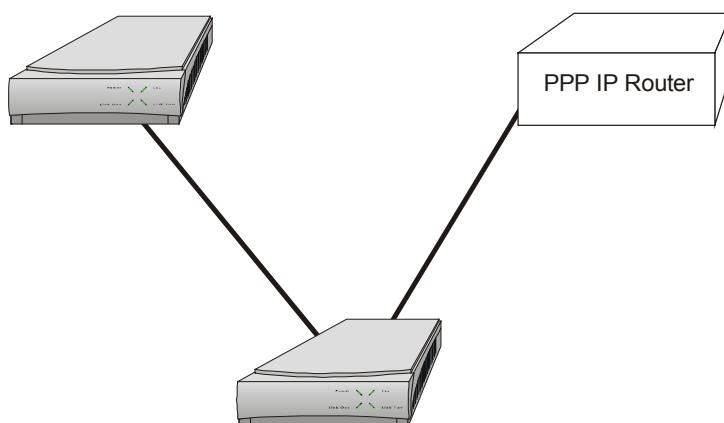


Figure 2 -9 Basic PPP Leased Line Configuration

The following steps must be performed on each of the routers in the network.



Local IP Address

Location: Main

- ↳ Configuration
- ↳ Interfaces Set-up
- ↳ LAN Set-up
- ↳ LAN IP Set-up
- ↳ *IP Address / mask size*

This is the IP address and subnet mask for the link of this router in the unnumbered IP connection.

Usually the clocking signal is received from the link (see Appendix D - Link Clocking Information). If the link interface is a V.11, V.35 or RS232 connection and the link speed is different from the default (64Kbps), and the router is to be the clock source, the link speed must be set to the clock speed that the router receives from the DCE link device.



Link Speed

Location: Main

- ↳ Configuration
- ↳ Interfaces Set-up
- ↳ WAN Set-up
- ↳ Link Set-up
- ↳ *Link Speed*

Bridge Connection

Once the link speeds have been configured, the router will attempt to establish the link connection to the remote site PPP router. The Bridge connection does not require any configuration for operation.

IP Router Connection

Once the link speeds and local IP address have been configured, the router will attempt to establish the link connection to the remote site PPP router. The IP connection is an unnumbered connection that requires only the configuration of the IP address of the router.

IPX Router Connection

Once the link speeds have been configured, the router will attempt to establish the link connection to the remote site PPP router. The IPX connection is an unnumbered connection that does not require any configuration.

If security is required for the direct dial connection refer to the Configure PPP Security section for information on setting the security passwords and user names for PPP.

Configure Remote Site Profiles

Remote Site Profiles allow the router to have different sets of configuration parameters for each of the remote site routers that may be called or that may call this router. This allows complete control over the configuration of each possible connection.

Each remote site profile is assigned an identification number when it is created, whether it is created automatically under auto-learning or manually by the user editing the remote site profile. The remote site is also named with an alias, which provides a more descriptive identifier for the remote site profile. For example, a remote site profile may be created with a name that describes the location of the remote router or a user name on an incoming connection. The alias may be up to 16 characters long and must begin with an alphabetic character (blanks and the character "!" are not allowed).

There can be up to 128 remote site profiles. The ID numbers are assigned automatically in ascending order as the site profiles are created.

ID numbers 129, 130 and 131 are templates for creating remote site profiles with ISDN, Frame Relay or Leased Line connections respectively. A template may have its parameters set to match common network configurations and then be used to quickly set-up a new site. In addition to the reserved templates, you can use any remote site as a template to create a new site.

The remote site profile allows the definition of various connection parameters: Circuit set-up, Bridge and Routing protocol configuration, activation criteria and security.

The following steps must be performed on the P1705 & P1730 in order to define a new remote site profile.



Remote Site Profile ID & Alias

Location: Main

- ↳ Configuration
- ↳ Connections up
- ↳ Remote Site Set-up
- ↳ Edit Remote Site

The remote site alias must be entered. The remote site profile is then created, an ID number is automatically assigned to it and the remote site profile is opened for editing. If a remote site profile already exists, either the ID number or the alias may be provided to access the site profile for editing.

Configure Remote Site Profiles for ISDN PPP

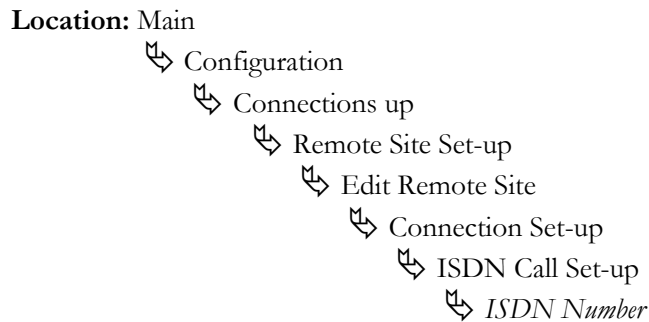
If this router is configured to have at least one ISDN switched circuit, the ISDN call parameters must be defined so that the router knows what ISDN phone number to dial when a connection to this remote site is required and what security parameters to use when establishing a connection.

When this router receives an ISDN connection it will prompt the calling device for a user name and password (PPP access security); once the name and password have been authenticated, the user name is used to search the remote site profile entries to find a match. Once a match is found, the configuration parameters defined within that remote site profile are used to finish establishing the PPP connection. For example, if this router receives an ISDN call from another device and in response to the user name prompt receives the name “Calgary”, it will look in the remote site list for a profile with the alias “Calgary”. If the “Calgary” profile is found, the parameters in it will be used for password authentication and completion of the connection. If there is no match for the user name “Calgary”, the call will be rejected.



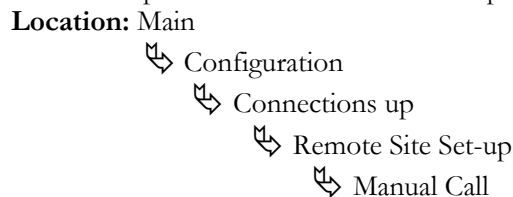
The remote site profile alias, user name of the security entry, and the user name defined on the partner PPP router must all be the same for the connection to be established.

Remote Site ISDN Phone Number



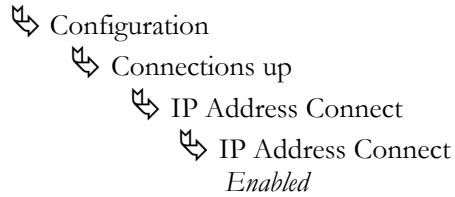
The ISDN number defined here is the ISDN phone number of the remote site ISDN PPP router. This is the ISDN phone number that will be dialed to establish a connection to this remote site profile. A connection to this remote site may be established by one of the following methods:

- 1 a) Using the Manual Call option of the Remote Site set-up menu,



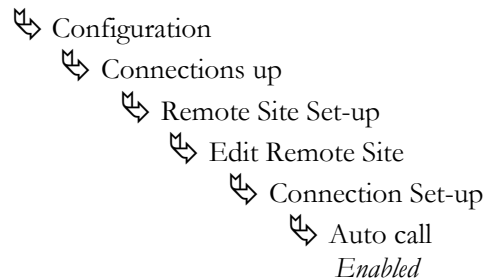
- 1 b) Defining this remote site profile within the IP Address connect table, which will cause a call to be made when a packet for this IP address is routed,

Location: Main



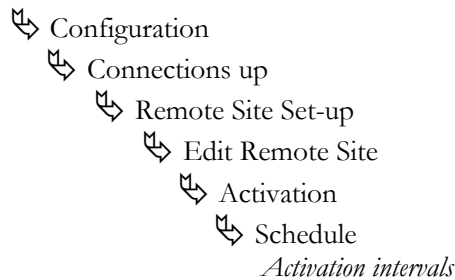
- 1 c) Defining the Auto-Call option within the Edit Remote Site menu of this remote site profile. (The Auto-Call option causes the router to attempt to establish a connection to this remote site profile each time the router starts up.)

Location: Main



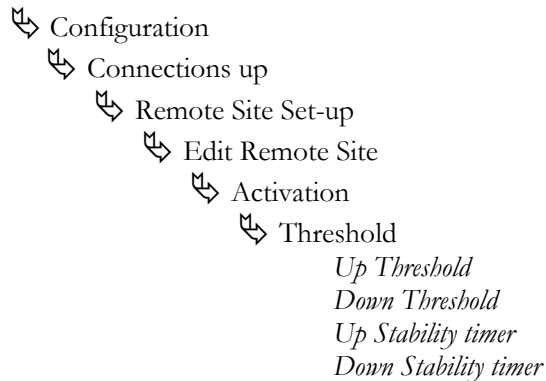
- 1 d) Setting up an activation schedule with times the connection is to be activated and deactivated

Location: Main



- 1 e) If a second ISDN channel is available and traffic level is enabled, setting the traffic load at which the second channel is to be activated.

Location: Main



Configure Remote Site Profile for Frame Relay

Each of the PVC's on the frame relay service must be configured within an individual remote site profile on the router. This is usually done automatically through the auto-learning process. When the frame relay router first starts up it will query the frame relay service to try to determine the PVC configurations. If the DLCI numbers of the PVC's on your service are determined during startup, the router will automatically create a remote site profile for each PVC. The automatically created remote site profiles will be named "LinkxDLCIyyy" where x is the physical link number the PVC is on and yyy is the DLCI of the PVC.



If during this learning process the maximum number of remote sites has been reached, the router will prompt you that there are no remote sites available. A new remote site cannot be auto-created unless one of the existing remote sites is manually deleted.

These automatically created remote site profiles may be renamed for easier identification or usage by changing the Remote Site Alias.



Remote Site Profile Alias

Location: Main
 ↳ Configuration
 ↳ Connections up
 ↳ Remote Site Set-up
 ↳ Edit Remote Site
 ↳ Remote Site Alias

Configuration: When configuring the router to use PAP or CHAP security authentication, after the router has automatically created remote site profiles for each of the PVC's, either the remote site profile alias must be changed to match the Outgoing User Name configured on the remote site router or vice versa. If the local remote site alias and the remote site routers outgoing user name do not match, the PVC will always fail with a security violation. Also note that PPP encapsulation must be enabled to run security access authentication.

With auto-learning, the above is all that is required of the user to set-up frame relay remote site profiles. If desired, parameters may be entered manually as follows:

Each PVC defined on this router must have a DLCI (Data Link Connection Identifier) value assigned for proper frame relay communication.



DLCI

Location: Main
 ↳ Configuration
 ↳ Connections up
 ↳ Remote Site Set-up
 ↳ Edit Remote Site
 ↳ Connection Set-up
 ↳ DLCI

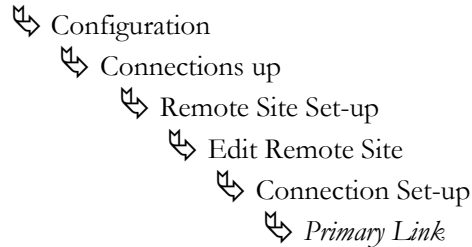
The DLCI number defined here is the Data Link Connection Identifier value provided by your frame relay service provider. This value **must** be set if auto-learning is disabled.

Each Remote Site PVC must be defined to exist on one of the two physical WAN links available on this router.



Primary Link

Location: Main



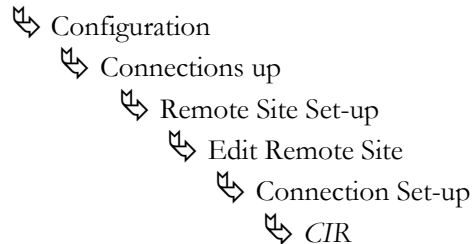
The Primary Link value defines to which of the two physical WAN links that this PVC will be assigned. This value **must** be set.

Two other values must be set before the remote site profiles are fully configured, the CIR and EIR. The Committed Information Rate (CIR) option specifies the data rate that the Frame Relay service has guaranteed to provide. The Excess Information Rate (EIR) option specifies the data rate that the Frame Relay service indicates may be available for this PVC.

CIR



Location: Main



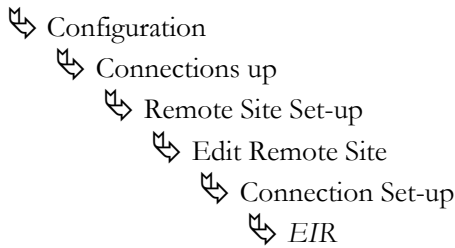
The CIR value specifies the guaranteed data rate for this PVC. This value **must** be set to the same as the value provided by the Frame Relay network provider. The value of 0 indicates that there is no commitment on the data rate.

Configuration: When changing the CIR option for this PVC, the PVC must be disabled and
Note then enabled before the new value will take effect.

EIR



Location: Main



The EIR value specifies the indicated data rate that may be available for this PVC. This value **must** be set to the same as the value provided by the Frame Relay network provider. When EIR = 0, no excess burst data is allowed to be transmitted. If EIR is non-zero, bursting is allowed. The only restriction is that CIR + EIR > 0.

Configuration: When changing the EIR option for this PVC, the PVC must be disabled and then enabled before the new value will take effect.

Note

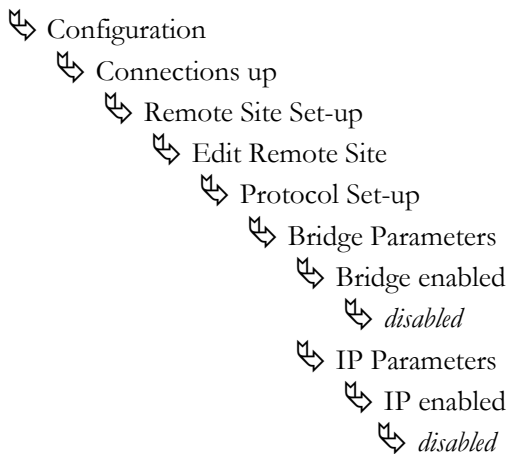
The Bridge, IP, IPX, and Compression settings may now be configured within the Bridge, Parameters, IP Parameters, IPX Parameters, and CCP Parameters menus (note: compression over frame relay is only available if PPP encapsulation is enabled).

If either the Bridge portion or the IP or IPX router portion of the connection is not required, the appropriate Connection Protocol setting must be disabled within the appropriate sub-menu. For example; if an IPX only connection is to be established, the Bridging and IP parameters must be disabled so that the router does not negotiate the Bridge or IP Connection Protocols on the connection.



Connection Protocol Setting

Location: Main



Disabling a particular connection protocol option will prevent the router from negotiating that Network Connection Protocol. Leaving all options enabled will result in a Bridge, IP router, and IPX router connection.

Configure Remote Site Profiles for Leased Line PPP

Remote Site Profiles allow the router to have different sets of configuration parameters for each of the possible remote site PPP routers that may be connected to this router. This allows greater control over the configuration of each possible PPP connection.

Each remote site profile is named with an alias. The alias provides a simple method of maintaining configuration control over the remote site profiles defined. For example, a remote site profile may be created with a name that describes the location of the remote PPP router. The alias also provides a method of matching a remote site profile and its configuration settings to a particular user name on an incoming connection. When a PPP security user name is defined the same as one of the remote site profiles, that remote site profile will be used for PPP negotiations after the security authentication process has passed. In other words, when this router receives a link connection attempt it will prompt the remote device for a user name and password (PPP security). Once the name and password have been authenticated, the user name is used to search the remote site profile entries to find a match. Once a match is found, the configuration parameters defined within that remote site profile are used to finish establishing the PPP connection.



The outgoing user name in the remote site security parameters entry, and the remote site alias defined on the partner PPP router must be the same to allow for proper operation.

The following steps must be performed on the P1705 & P1730 in order to define a new remote site profile.



Remote Site Profile ID & Alias

Location: Main

- Configuration
- Connections up
- Remote Site Set-up
- Edit Remote Site

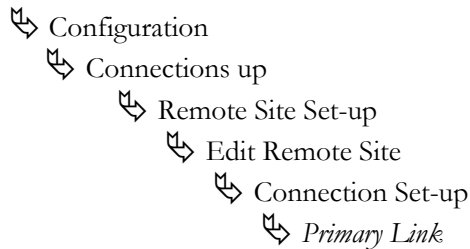
The remote site alias must be entered to create a new site. If a user defined remote site profile already exists, only the id number needs to be provided to edit that site's parameters.

Now that the remote site profile is created, a link number must be assigned as the primary link number. The primary link number is the link interface that the router will use to attempt to establish a connection to the remote site PPP router.

Primary Link Number



Location: Main



The Primary Link number defined here is the link interface used to establish the connection to the remote site PPP router. When a link number is defined within a new remote site profile, that link number will be removed from any remote site profile that originally was defined to use the link. The link will then be used within the newly defined remote site profile.

When this remote site profile is defined to use Multilink protocol, the Secondary Connection should also be defined.

The Bridge settings may now be configured within the Bridge Parameters menu.

The IP settings may now be configured within the IP Parameters menu.

The IPX settings may now be configured within the IPX Parameters menu.

The Compression settings may now be configured within the CCP Parameters menu.



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the PPP Menu Reference Manual file on the accompanying CD-ROM.

Configure Remote Site Profiles for Frame Relay with ISDN backup

Frame Relay operation is set-up as described in section 2.3.2



The PVC on both partner routers must be disabled during this set-up procedure, then re-enabled when ready to start.

ISDN call set-up is done as described in section 2.3.1.

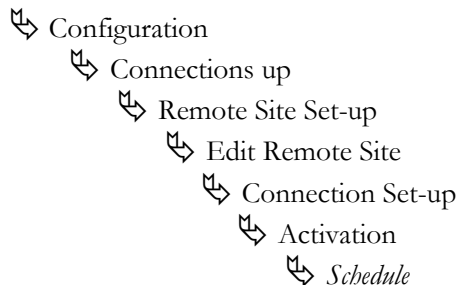
Recovery operation is set-up on the secondary activation menu.

If the ISDN circuit is to be available only at specified times, rather than all the time (the default), set-up a recovery schedule with times the connection is to be activated and deactivated



Activation Schedule

Location: Main



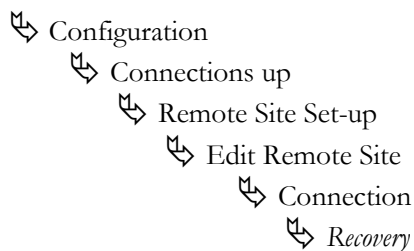
Enter “a” and the times the recovery circuit is to be made available, enter “d” and the times the recovery circuit is to be deactivated.

Enable the secondary activation circuit for recovery



Recovery

Location: Main



The recovery schedules MUST be set identically on both partner PPP routers to operate; if they are not, one router will try to bring the link up and the other will shut it down.

Configure Remote Site Profiles for PPPoE

Remote Site Profiles allow for the router to be configured to support PPP over Ethernet (PPPoE) client on the router. The PPPoE feature on the Perle routers provides a PPPoE client support on Ethernet interfaces to a bridging DSL modem to the Internet. This feature will create a PPP tunnel to an ISP located somewhere on the ATM network side of the xDSL modem. This feature eliminates the hassle and potential error of running a PPPoE client on each LAN workstation that requires Internet access. This feature is only available on the Perle 1730 model.

The following steps must be performed in order for the router to be configured for PPPoE connection. The remote site set-up for the PPPoE should refer to the section for Configure Remote Site Profiles for Leased Line PPP as the initial guideline for setting up a remote site configuration for PPP. Afterwards the following steps transform the PPP remote site connection to a unique PPPoE remote site configuration.

Location: Main

- ↳ Configuration
- ↳ Connection Set-Up
- ↳ Remote Site Set-up
- ↳ Edit Remote Site
- ↳ Connection Set-up
- ↳ Primary Link
- ↳ LAN

The Primary Link options will display two options LAN1 and LAN2 if the unit detects the secondary LAN Interface module installed.

The Auto-Call field will be automatically setup to be enabled when a LAN interface is selected as the primary link. This will allow the PPPoE connection to be established automatically upon boot-up of the router.

To verify that PPPoE is enabled for this remote connection, view the read-only parameter

Location: Main

↳ Configuration
↳ Configuration
↳ Connection Set-UP
↳ Remote Site Set-Up
↳ Edit Remote Site
↳ Protocol Set-Up
↳ PPPoE
↳ *enabled*

When setting up your PPPoE link with your ISP provider, one global IP addresses will be provided that should be used for the PPPoE remote site configuration. By enabled the NAT feature on the remote site configuration allows you to maintain only one global IP addresses for all PC workstation on your internal LAN.

Location: Main

↳ Configuration
↳ Connection Set-up
↳ Remote Site Set-Up
↳ Edit Remote Site
↳ Protocol Set-Up
↳ IP Set-up
↳ NAT enabled
↳ *enabled*

Access to some web pages is a common problem experienced when running a PPPoE client on a router. By design, PPPoE packets can support a maximum MTU of up 1492 bytes. Normally when a connection is established over common PPP, the TCP protocol negotiates its maximum data size using the mss option (default 1460). By default, most Windows PCs have their TCP mss option set to 1460 bytes. Since PPPoE requires an additional 8 bytes of header data, the TCP mss option should decrease to 1452 bytes. Therefore when configuring the router for PPPoE, the remote site NAT configuration automatically adjust its TCP mss option to 1452 to accommodate this requirement. To verify this value has been adjusted:

Location: Main

- ↳ Configuration
 - ↳ Connection Set-Up
 - ↳ Remote Site Set-up
 - ↳ Protocol Set-Up
 - ↳ IP Parameters
 - ↳ NAT Advanced Set-up
 - ↳ TCP mss
 - ↳ *enabled*
 - ↳ TCP mss value
 - ↳ *1452*

Normally your ISP provider will provide you with an outgoing username and password and to authenticate with their services. The PPPoE remote site configuration needs to have the security section configured with this ISP parameters to authenticate the PPPoE connection.

Location: Main

- ↳ Configuration
 - ↳ Connection Set-Up
 - ↳ Remote Site Set-Up
 - ↳ Security Set-Up
 - ↳ Outgoing Username
 - ↳ *ISP provided username*
 - ↳ Outgoing PAP password
 - ↳ *ISP provided password*
 - ↳ Outgoing CHAP password
 - (if required by ISP)
 - ↳ *ISP chap password*

To ensure that network traffic is routed to the PPPoE connection, the router must be configured to have the default IP gateway setup to your newly created PPPoE remote site connection.

Location: Main

↳ Configuration

↳ Packet Services

↳ IP Routing Set-up

↳ IP Gateway

↳ *PPPoE remote site alias*

Advanced Features

Configure Dynamic Host Configuration Protocol

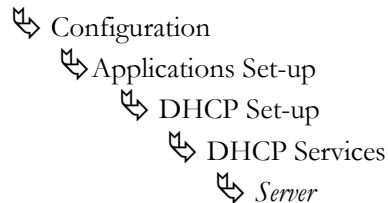
The P1705 & P1730 use Dynamic Host Configuration Protocol (DHCP) to allow users in a small office environment to be added and removed from a network with all of the network information (i.e. IP address, DNS, subnet mask, etc.) being configured automatically. DHCP configures devices (DHCP clients) from a central DHCP server. It is designed to allocate network addresses to a number of hosts on the router's LAN and supply the minimal configuration needed to allow hosts to operate in an IP network.

The following steps must be performed on the P1705 & P1730 to configure it as a DHCP server.



DHCP Services

Location: Main

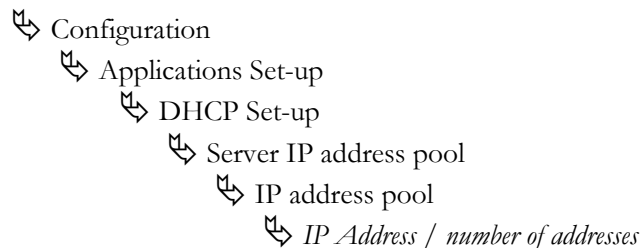


DHCP Services options which are available are none, relay and server. Set to server to enable this device as a DHCP Server.



IP Address Pool

Location: Main



The IP address pool option requires setting the first IP address in the range that is to be used for the devices attached to the DHCP Server. The number of addresses to be assigned must also be specified, to a maximum of 253.



When setting up a router as a DHCP server, you may not assign an address pool that includes broadcast addresses (all ones in the host portion of the IP address) for known networks. Known networks include any local networks plus standard A, B and C class addresses.

With the DHCP Services and IP Address Pool defined, devices may be attached to the network (up to the maximum specified) and they will be automatically configured.



When setting up a router as a DHCP server that will have both a DNS server on the internal network and a remote connection to another DNS server (for example, through an ISP), then the local DNS server should be set as the primary DNS and the external DNS server as the secondary DNS.



DNS Set-Up

Location: Main

↳ Configuration

↳ Application Set-up

↳ DHCP Set-up

↳ DNS Set-up

↳ Primary DNS

-IP address local DNS server

↳ Secondary DNS

-IP address external DNS server

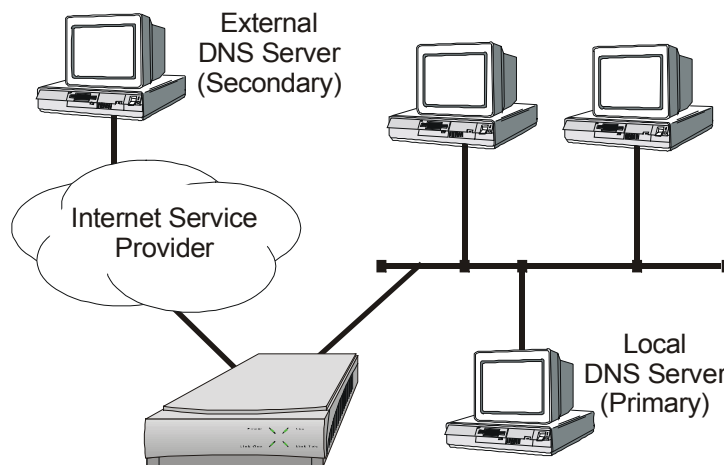


Figure 2 -10 Local + External DNS Server Configuration



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the PPP Menus Manual file on the accompanying CD-ROM.

Network Address Translation and Port Translation

The P1705 & P1730 provide support for Network Address Translation (NAT). Network Address Translation is a technique that translates private IP address on a private network to valid global IP addresses for access to the Internet. Network Address Port Translation (NAPT) translates both the IP address and the port number. The advantage of port translation is that more than one private IP address can be translated to the same global IP address. Port translation allows data exchanges initiated from hosts with private IP addresses to be sent to the Internet via the router using a single global IP address. A global IP address must be assigned to the WAN link upon which NAPT is enabled for port translation to work. The global IP address will be assigned by the ISP.

To use NAPT, the private network addresses of the services that will be available globally must be assigned:



NAT Exports

Location: Main

- Configuration
- Applications Set-up
- NAT Exports
- Edit Services
- *enter the private network IP address of each service offered*

Then NAT (Network Address Translation) is enabled:



NAT Enable

Location: Main

- Configuration
- WAN Set-up
- Remote Site Set-up
- Edit Remote Site
- Protocol Set-up
- IP Parameters
- NAT Enabled
- Enabled*

Configuration: When running frame relay RAW 1490, the local IP address and peer router IP address must be set in the IP parameters menu.

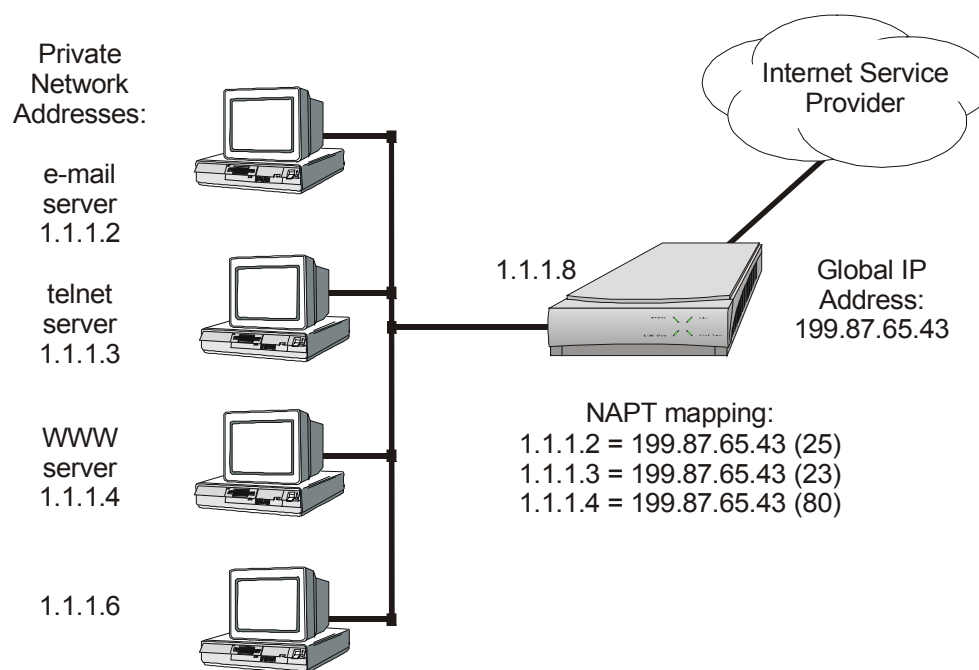


Figure 2 -11 NAT Configuration

Security

The router provides a number of means of providing security on incoming and outgoing traffic on a network. These methods include the IPsec protocol suite, access password authentication, firewall limiting access to only designated device addresses, private network address translation (NAT) and filtering for both incoming and outgoing traffic.

IPSec Protocol Suite

The PPP P1705 & P1730 support a number of features from the Internet Protocol Security (IPSec) extensions that provide data encryption, authentication and privacy. IPSec can be used to establish a secure Virtual Private Network (VPN) over a public network. The connection through the unsecured public network between two routers on a VPN is often referred to as a “tunnel”.

A VPN is set-up as a Security Association (SA) between the two routers (also known as security gateways in this case) on either end of the desired secure connection. The SA defines the security parameters that will be used between the two routers. Many of the settings define “source” and “destination” parameters. These settings will be mirror images on the partner routers; i.e. the “source” value for a parameter will become the “destination” setting when configuring the partner router.

Each router on the VPN has a policy list which defines the SAs, the IPSec authentication and encryption parameters, and the rules used to determine which packets are passed through the interface. The IPSec policy is applied at the outbound interface of the router and packets enter the tunnel at the outbound interface.

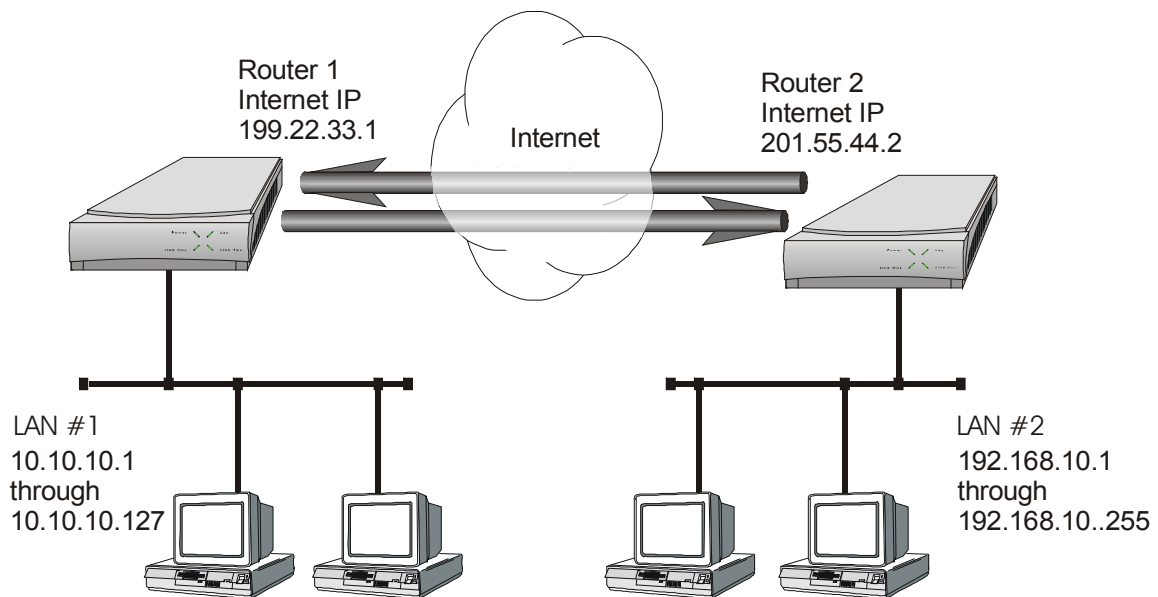


Figure 2 -12 Sample IPSec Application

The figure above illustrates an example of a VPN made up of two private address LANs joined through the Internet by IPSec tunnels from router 1 to router 2 and router 2 to router 1. The routers are set-up with numbered links, so that each router's Internet connection has a publicly known address that is separate from the private LAN IP address for that router. Note that this example does not

make provision for NAT to be used with tunneling. We will use this example for the configuration on the pages that follow.

The setup for an IPSec connection is done in the IP security set-up menu under Configuration - Packet Services. IP Security may be disabled to check the link connections before the secure connection is set-up.



Security Level

Location: Main

- ↳ Configuration
- ↳ Packet Services Set-up
- ↳ IP Security Set-up
- ↳ *IP Security*

Be sure to toggle IP Security back to enabled when IPSec is configured.

Each data packet that goes through an IPSec router will be tested against one or more sets of rules concerning the source IP Address of the packet, the destination IP Address of the packet, the IP protocol (TCP, UDP, etc.) associated with the packet, the source port from which the packet originated and destination port to which it is going. An action determined by the outcome of the test is then performed on the packet (such as IPSec processing, discard, etc.).

The first step in setting up IPSec is to define the local address that the router will use for the local end of the tunnel (SA)



IPSec Policy Set-up

Location: Main

- ↳ Configuration
- ↳ Packet Services Set-up
- ↳ IP Security Set-up
- ↳ Policy Set-up
- ↳ Local IP address
- **199.22.33.01**

The Local IP Address must be an IP address for this router on the public network. It should not be a dynamically assigned address. In this case Router 1's address will be the numbered WAN link 199.22.33.01. If this connection had been set-up as an unnumbered link, then the local IP would be set as "LAN" or the router's IP address. Note that in the case of unnumbered links, the LANs would require registered IP addresses to operate over the Internet.

The policy is applied at the WAN link (the outbound IPSec interface), this must be specified



IPSec Policy Set-up

Location: Main

- ↳ Configuration
- ↳ Packet Services Set-up
- ↳ IP Security Set-up
- ↳ Interfaces Set-up
- ↳ IPSec Interface
- WAN*

Note that the policy will be applied to all WAN interfaces, so a link on a second WAN interface must have a policy item (or items) to permit traffic across that interface.

Next, the policy item(s) that specify the SA(s), the rules to test packets against and encapsulation algorithms and keys must be set. Each policy item is created by entering a name after selecting the Edit Item menu option.



IPSec Policy Table Entry

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - item_name*

The name may be up to 16 alphanumeric characters; spaces are not allowed, use underscore as a separator.

After the name is entered, the Edit Policy Item menu will be displayed. Under this menu the Encapsulating Security Payload SA parameters and policy rules are set.



IPSec ESP SA

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - item_name*
 - ↳ Manual ESP SA
 - ↳ Peer IP Address
 - 201.55.44.02
 - ↳ Outbound SPI
 - 24680BD
 - ↳ Inbound SPI
 - ECA97531

The Security Parameters Indices (SPI) are identification numbers used to identify packets to (outbound) or from (inbound) the peer router in the SA connection. The Outbound SPI on one router must be exactly the same as the Inbound SPI on the peer; similarly the Inbound SPI must exactly match the outbound SPI on the peer set-up. The example shows 8 hex character SPIs as set in Router 1, so for Router 2, the matching Outbound SPI would then be ECA97531 and the Inbound SPI 24680BD.

Then the authentication algorithm should be set to MD5



IPSec ESP SA

Location: Main

- ↳ Configuration

- ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - item_name*
 - ↳ Manual ESP SA
 - ↳ Authentication
 - MD5*

If Authentication is left as “none” (the default setting), no authentication will be done on the packet, only encryption will be performed.

Next, the encryption and authentication keys are Set-up. As with the SPIs, the Inbound-Outbound pairs must be mirrored on the peer router set-up.



IPSec ESP SA

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - item_name*
 - ↳ Manual ESP SA
 - ↳ Keys
 - ↳ Outbound encrypt key
 - 0123456789ABCDEF*
 - ↳ Inbound encrypt key
 - FEDCBA9876543210*
 - ↳ Outbound auth key
 - 1F1F1F1F1F1F1F1F1F1F1F1F1F1F1F1F*
 - ↳ Inbound auth key
 - F1F1F1F1F1F1F1F1F1F1F1F1F1F1F1F1*



The encryption keys must be exactly 16 hex characters for DES encryption (48 hex characters for 3-DES) and the authentication keys must be exactly 32 hexadecimal characters long.

Typical Applications & How to Configure Them

Now the selection rules used to test each packet against are set



IPSec ESP SA

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - item_name*
 - ↳ Selection Rules
 - ↳ Src IP
 - 10.10.10.1 (25)
 - ↳ Dest IP
 - 192.168.10.1 (24)
 - ↳ Protocol
 - any
 - ↳ Src port
 - any
 - ↳ Dest Port
 - any

The example policy items for Router 1 show the source and destination specified by the local IP addresses with masks. All protocols will be allowed between all ports.

Then the policy item must be activated.



IPSec ESP SA

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - item_name*
 - ↳ Activate

If packets are to be checked against more than one policy item, tab back to the Policy set-up menu and repeat the previous steps for the next policy item. There may be up to 32 policy items. Packets are tested against policy items in order of the items' priority numbers, from lowest to highest.

To do its job as a router, this device must know where to forward packets with IP addresses outside the LAN. This may be done in a number of ways: a static IP route to the LAN at the other end of the SA connection may be set, the IP address of the Internet Service Provider may be set as the Default Gateway, or an IPSec policy item may be created specifically to pass RIP packets.

To set a policy item for RIP packets, first set the action to bypass IPSec so the packets are not processed.



IPSec ESP SA

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - pass_RIP*
 - ↳ Action
 - bypass_IPSec*

then set up the rules to check for RIP packets



IPSec ESP SA

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item
 - pass_RIP*
 - ↳ Selection Rules
 - ↳ Src IP
 - any*
 - ↳ Dest IP
 - any*
 - ↳ Protocol
 - 17*
 - ↳ Src port
 - 520*
 - ↳ Dest Port
 - 520*

RIP packets (protocol 17 - UDP) to and from any IP and to and from port 520 will be passed through the WAN interface on this router.

Typical Applications & How to Configure Them

Once the IPSec policies have been configured and it has been confirmed that traffic is passing over the IPSec connection, the default action for failed packets should be changed to discard. The initial factory setting is to bypass IPSec, which allows remote configuring of the router via Telnet. Once the IPSec configuration has been completed and tested, this should be changed so that only those packets matching the IPSec conditions are passed.



IPSec Policy Set-up

Location: Main

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Default action
 - discard*



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P1705 & P1730 VPN Menus Manual file on the accompanying CD-ROM.

Internet Key Exchange (IKE)

The IKE feature is designed to automatically negotiate IPsec security associations (SAs) and enables IPsec secure communications without costly manual preconfiguration. IKE provides also authentication of the IPsec peers and generate keys to be used by IPsec. Phase 1 is to establish a secure and authenticated tunnel with which to communicate further IKE negotiations. Phase 2 is to establish security associations (SA) on behalf of other protocols like IPsec which require key and parameter negotiation.

In order for IPsec to be negotiated dynamically across an IKE connection the IPsec policy item must be linked to IKE protection suite. An IKE protection suite defines the IPsec SA parameters which are negotiated

To initially configure the IKE parameters for Phase 1 negotiation, you need to configure the router as follows. NOTE: Phase 1 can support up to 3 proposals negotiated during IKE negotiation with proposal 1 considered the first to negotiate:

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ IKE peer setup
 - ↳ Peer alias
 - ↳ *Peer name*
 - ↳ Peer IP Address
 - ↳ xxx.xxxx.xxx.xxx
 - ↳ Peer Pre Shared Key *
 - ↳ Peer Public Key *
 - ↳ IKE Phase 1 Negotiation
 - ↳ *Authentication Method*
 - ↳ *Integrity*
 - ↳ *Encryption*
 - ↳ *DH Group*
 - ↳ *Lifetime*
 - ↳ *Proposal*

*Note - Either Pre-Shared Key or Public Key can be used for implementation but not both.

To configure the router for IPsec to be negotiated through IKE you must defined the IKE protection suite to be establish during Phase 2:

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Protection Set-up
 - ↳ Edit Protection Suite
 - ↳ Suite Alias
 - ↳ *Protection Suite name*
 - ↳ SA mode
 - ↳ *IPSEC SA mode*
 - ↳ Lifetime for SA (seconds) OR
 - ↳ Lifetime for SA (data)
 - ↳ *Lifetime value*

Typical Applications & How to Configure Them

- ↳ Transform-1
 - ↳ *Encryption/Authentication 1*

To link an IPSec policy item to an IKE tunnel, the following items are required to be changed in an existing IPSec policy item. The IPSec policy item must indicate that the IPSec SA is to be negotiated through the IKE SA and specifically which IKE protection suites are to be used.

- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Local IP Address
 - ↳ *IP Address of this router*
- ↳ Configuration
 - ↳ Packet Services Set-up
 - ↳ IP Security Set-up
 - ↳ IPSec Interface
 - ↳ *WAN*
 - ↳ Policy Set-up
 - ↳ Edit Item Menu
 - ↳ *Item name*
 - ↳ SA Creation
 - ↳ *IKE*
 - ↳ IKE ESP SA
 - ↳ Peer IP Address
 - ↳ *Peer IP Address*
 - ↳ IKE PFS
 - ↳ IKE SA Proposal
 - ↳ Protection Suite 1
 - ↳ *Alias for IKE protection suite 1*
 - ↳ Protection Suite 2
 - ↳ *Alias for IKE protection suite 2 (optional)*
 - ↳ Protection Suite 3
 - ↳ *Alias for IKE protection suite 3 (optional)*

- ↳ Configuration
 - ↳ Packet Service Set-up
 - ↳ IP Security Set-up
 - ↳ Policy Set-up
 - ↳ Edit Item Menu
 - ↳ Selection Rules Menu
 - ↳ Edit Service
 - ↳ Source IP Address
 - ↳ Destination IP Address
 - ↳ Protocol
 - ↳ Source Port
 - ↳ Destination Port

Configure PPP Security

The PPP P1705 & P1730 provide support for both PAP and CHAP security access authentication. An outgoing user name, PAP password, and CHAP secret are defined that the router will use when responding to an authentication request from a remote site PPP router.



The cold start defaults for the security user name and passwords are as follows. These defaults will exist when the router is first started before and configuration is entered, and after a Full Reset has been performed. These default values are also set when the router is placed in TFTP Network load mode for upgrading the operating software via TFTP transfers. Care should be taken when upgrading a group of routers that have security levels set.

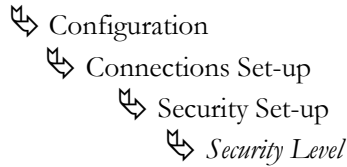
Default outgoing user name for each remote site when it is defined is the same as the default device name. Default PAP password and CHAP secret are both set to "BRIDGE".

The complete password security configuration for both incoming and outgoing calls is defined within the Security menu of the WAN set-up section.



Security Level

Location: Main



The security level defines the type of security that this router will request when a remote site PPP router attempts to establish a PPP connection. The security may be defined as none, PAP, or CHAP.

When a security level is defined on this router, an entry for each remote site PPP router that may be connected to this router **must** be placed in the security database. The security database is used to store the user names and passwords of the remote site PPP routers.



Remote Site Security Parameters Entry

Location: Main

- ↳ Configuration
- ↳ Connections up
- ↳ Edit Remote Site
- ↳ Security Parameters
 - ↳ Outgoing User Name
 - ↳ Incoming PAP Password
- ↳ Outgoing PAP Password

or

- ↳ Incoming CHAP Secret
- ↳ Outgoing CHAP Secret

The outgoing entries in the security database define the user names and passwords/secrets that this router will send in response to an authentication request is sent from the remote partner router. The incoming entries define the passwords/secrets that this router expects to receive from the remote partner in response to authentication requests.



For a pair of partner routers with security enabled, the outgoing user name in the security parameters entry of one router must match the remote site alias in the partner router's remote sites table.



To use PPP security with frame relay, PPP encapsulation must be enabled. The PVC must be disabled to change the PPP encapsulation status, then re-enabled.



The configuration options described here are only for initial set-up and configuration purposes. For more complete information on all of the configuration parameters available please refer to the P1705 & P1730 VPN Menus Manual file on the accompanying CD-ROM.

Configure Firewall

The P1705 & P1730 provide Firewall security for restricting access between any two networks connected through the router. Firewalls are set-up on a per connection basis for the LAN and remote sites. The direction of filtering is from the perspective of the router; incoming traffic is from the network in question to the router, outgoing is from the router to the network. The direction of filtering may be set to incoming, outgoing, both or none. Once the direction of filtering for a connection has been set, holes may be created in the firewall to allow specified traffic through. Normally, the LAN firewall is used for restricting intranet traffic (connections within the corporate network) and remote site firewalls are used to limit access from less trusted sources, such as the Internet or dial-up ISDN links.

The following diagram shows a corporate head office network, which is connected, to the Internet with an router. There is also a branch office at a remote site connected with a leased link. The administrator at the corporate head office wishes to set-up an IP firewall to allow everyone on the Internet to have access to the corporate FTP and Web servers and nothing else. The administrator also wishes to allow all of the TCP traffic from the branch office network to have access to the head office. Anyone in the corporation may have unrestricted access to the Internet.

Main FTP server: 195.100.1.12
Main Web server: 195.100.1.20

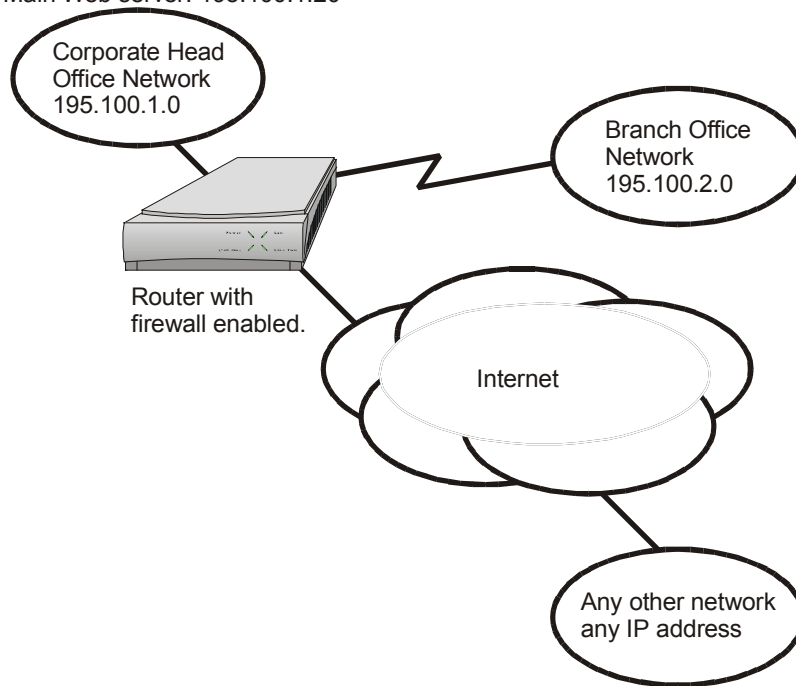


Figure 2 -13 Sample Firewall Application

The following steps must be performed on the P1705 & P1730 to set-up the firewall support as desired.

First the firewall on the ISP connection (remote site 1) of the WAN is set-up. The firewall option is set to “inbound” to have this WAN firewall filter traffic from the ISP to the router while allowing unrestricted access out to the Internet.



Firewall

Location: Main

- ↳ Configuration
- ↳ Applications Set-up
- ↳ Firewall Set-up
- ↳ WAN Firewall Set-up
 - ↳ *enter ID# 1 for ISP remote site*
 - ↳ Firewall
 - ↳ *inbound*

The firewall on the Internet connection is set-up to protect the entire corporate network, including the branch office, from unauthorized traffic.

Then the entries are made in the “Designated Servers” menu to allow Internet access to the FTP and Web servers on the corporate network.



FTP & WWW Designated Servers

Location: Main

- ↳ Configuration
- ↳ Applications Set-up
- ↳ Firewall Set-up
- ↳ WAN Firewall Set-up
 - ↳ *ID# 1 for ISP remote site*
 - ↳ Designated Servers
 - ↳ *FTP Server*
 - 195.100.1.12
 - ↳ *WWW (HTTP) Server*
 - 195.100.1.20

When defining a designated server you will be prompted for the IP address of that device. Adding an entry to the designated servers list allows you to quickly setup a firewall entry without having to figure out TCP port values.

Next, the LAN firewall is set-up to restrict access to the LAN. The firewall option is set to “outbound” to have the LAN firewall filter traffic from the router.



Firewall

Location: Main

- ↳ Configuration
- ↳ Applications Set-up
- ↳ Firewall Set-up
- ↳ LAN Firewall Set-up
 - ↳ Firewall
 - ↳ *Outbound*

Note: if this P1730 has a second LAN interface installed, you will be requested to select which LAN this firewall entry is to be used with.

Then an entry is placed in the firewall table to allow the devices in the branch office remote site to have unlimited TCP access to devices in the head office.



Firewall Table Entry

Location: Main

- ↳ Configuration
 - ↳ Applications Set-up
 - ↳ Firewall Set-up
 - ↳ LAN Firewall Set-up
 - ↳ Edit Firewall Entry
 - ↳ *filter ID # 1*
 - ↳ *Destination Address*
 - 195.100.1.0
 - ↳ *Destination Mask*
 - 255.255.255.0
 - ↳ *Source Address*
 - 195.100.2.0
 - ↳ *Source Mask*
 - 255.255.255.0
 - ↳ *Protocol Type*
 - TCP
 - ↳ *Entry Direction*
 - outbound

Finally, holes are provided in the LAN firewall to allow Internet access to the FTP and WWW servers



Firewall

Location: Main

- ↳ Configuration
 - ↳ Applications Set-up
 - ↳ Firewall Set-up
 - ↳ LAN Firewall Set-up
 - ↳ Designated Servers
 - ↳ *FTP Server*
 - 195.100.1.12
 - ↳ *WWW (HTTP) Server*
 - 195.100.1.20

***i** The configuration options described here are only for initial set-up and configuration purposes. For more information on all of the configuration parameters available please refer to the P1705 & P1730 VPN Menus Manual file on the accompanying CD-ROM.*

Network Address Translation

Using private addresses on a network and NAT/NAPT for interactions over an internetwork connection hides the internal address from the rest of the world. Access is restricted to only those services that are specifically designated to be available. Please see section 2.4.2 for more information on Network Address Translation.

Filters

The programmable filtering functions available on the P1705 & P1730 provide a very powerful means of controlling traffic flow to and from a network. Please see section 3 *Introduction to Filtering* for details on how to set-up various filtering operations.

Compression

Compressing data allows data throughput rate considerably greater than the physical line rate. The actual rate achieved will depend on how compressible the specific data is. Generally, graphics and databases compress up to 600%, text 400 to 500%, binary codes about 200%.

At line rates above 256 Kbps, compression is not effective as it takes more time to perform the compression than to transmit the raw data.



Enable compression

Location: Main

- ↳ Configuration
- ↳ Connections up
- ↳ Remote Site Set-up
- ↳ Edit Remote Site
- ↳ Protocol Set-up
- ↳ CCP parameters
- ↳ Compression
- ↳ *Enabled*

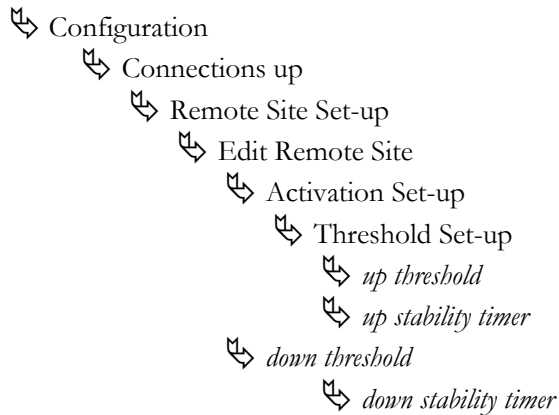
Bandwidth On Demand

The router may be set to activate its secondary link when the load on the primary link exceeds a user-defined threshold.



Set the traffic loads for enabling and disabling the secondary circuit

Location: Main



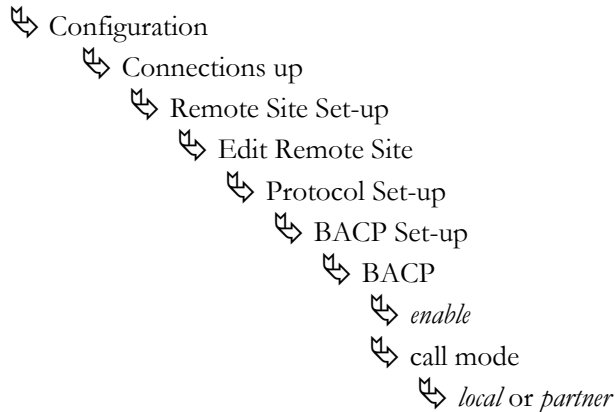
The up and down stability timers are the delay times that the primary link must be above the threshold before the secondary is activated or below threshold before it is brought down. This prevents activation or deactivation of the secondary link due to momentary peaks or drops in traffic.

Bandwidth Allocation Control Protocol (BACP) may be used to negotiate the link activation between partner routers (BACP must be used if the partner router is not another router).



Enable BACP

Location: Main



Call mode determines which router originates the call to bring up the second link.

If BACP is not used, the partner routers will use proprietary negotiations to determine which router is to activate the second link.

QOS - Priority Queuing

Priority Queuing (PQ) allows the users to configure the router to allow specific traffic bound for an outgoing interface to be prioritized into high, medium, normal and low queues. Packets sent to the high priority queue are serviced first, followed by the packets on the medium queue and so on. The router can configure outbound traffic to specific queues based upon protocol, addresses and incoming interfaces.

To enable Priority Queuing you must configure a Priority list which contains the criteria items for the outbound packets. Each packet will be compared to item #1 in the Priority List and then progress down the list of items in order until a match is found. When a match is found, the comparison search will stop and the packet will be given the priority configured for that item. Thus more specific priority criteria should be defined at the beginning of the list.

To define item criteria within a Priority List:



Location: Main

↳ Configuration

↳ Packet Services Setup

↳ QOS Setup

↳ Priority Queuing

↳ Edit Priority List

↳ Edit Items

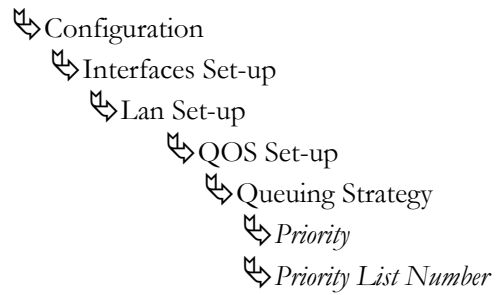
Once the Priority List is defined, the Priority List can be assigned to a Remote Site interface or the LAN interface.

Typical Applications & How to Configure Them

To assign a Priority List to a LAN interface:



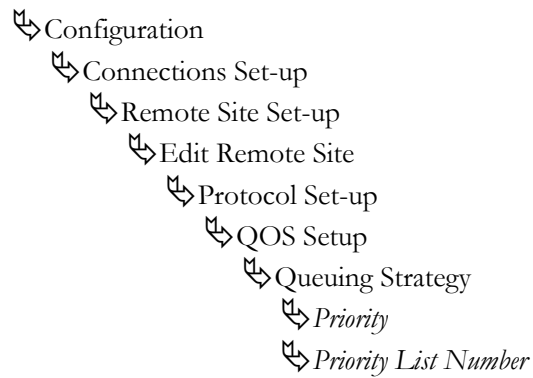
Location: Main



To assign a Priority List to a Remote Site Connection:



Location: Main



Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) feature on the Perle Routers support the client side of the protocol as described in RFC 2030. The router will be able to obtain its time from a NTP or SNTP server and then can be synchronized amongst other network devices. Additionally, the router can also be configured to support various time variations features such as local time zone and adjustments for daylight savings time.

When the Perle router has SNTP enabled it will periodically send NTP packets to the NTP/SNTP server which will respond with the network time. The router will synchronize its internal clock with the response from the NTP/SNTP server. The method in which the router sends or receives the NTP packets from the NTP/SNTP server is configurable in three modes: unicast, multicast and anycast.

In unicast mode, the router will have to be configured with the IP Address of the NTP server and will periodically send a request packet to the NTP server. The NTP server will then respond directly to this request with the current time. The Perle router supports a primary and a secondary IP Address for NTP servers.

In multicast mode, the router does not initiate the request packets but waits to receive the periodic broadcasts from the NTP server with the current time. Once the router receives an NTP packet from the server, it will then synchronize its internal clock with the current time.

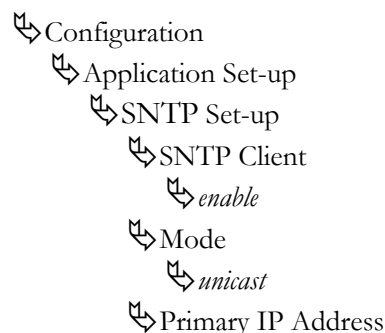
In anycast mode, the router will send out a request packet as a broadcast on the LAN to get a response from any NTP server. When the first response is received from an NTP server, the internal clock of the router is synchronized. The router will learn the IP Address of the NTP server that responded and then operate in unicast mode.

The Perle router supports time variation feature of local time zones and daylight savings time regardless if the internal clock is synchronized with an NTP server. The local time zone feature allows the router to offset the internal clock by a configurable time from the UTC time. The configurable time zone off set can be specified in hours (0 to 23) and minutes (0 to 59) and can also be specified by a specific name up to 4 characters.

Adjustments to the internal clock for daylight saving time (Summer-time) can be enabled and specified for one time within the year or recurring year after year. Configuration parameters allow the router to enable Summer-time each year by specifying the month, week, day and hour for the begin and end Summer-time.

To enable SNTP on the router and setup for unicast mode to directly obtain the time from a specific NTP server implement the following steps.

Location:



Typical Applications & How to Configure Them

- ↳ IP Address (*XXX.XXX.XXX.XXX*)
- ↳ Secondary IP Address
 - ↳ IP Address (*XXX.XXX.XXX.XXX*)
- ↳ Version
 - ↳ 3

The time zone and daylight savings time configuration is setup within the device setup menu. To configure for Eastern Standard Time (EST) and have daylight saving time implemented for this year only, implement the following steps:

Location:

- ↳ Configuration
 - ↳ Access Set-up
 - ↳ Device Set-up
 - ↳ Time Zone Setup
 - ↳ Hours Offset
 - ↳ 5
 - ↳ Minutes Offset
 - ↳ 0
 - ↳ Name
 - ↳ *EST*
 - ↳ Summer Time Setup
 - ↳ Summer Time
 - ↳ *enabled*
 - ↳ Summer Time Mode
 - ↳ *date*
 - ↳ Summer Time Start
 - ↳ *Year*
 - ↳ *Month*
 - ↳ *Date*
 - ↳ *Time*
 - ↳ Summer Time End
 - ↳ *Year*
 - ↳ *Month*
 - ↳ *Date*
 - ↳ *Time*
 - ↳ Offset
 - ↳ 60

3

Introduction to Filtering

The P1705 & P1730 provide programmable filtering which gives you the ability to control under what conditions Ethernet frames are forwarded from one network to another. There are many reasons why this might need to be accomplished, some of which are security, protocol discrimination, bandwidth conservation, and general restrictions.

Filtering may be accomplished by using two different methods. The first method is to filter or forward frames based solely on their source or destination MAC address. This method of filtering is useful when bridging between LANs and for providing remote access security in any type of network. The Ethernet MAC (Media Access Control) address is checked against the addresses in the filtering list and the frame is filtered or forwarded accordingly.

The second method of filtering is pattern filtering where each frame is checked against a filter pattern. The filter pattern may be defined to perform a check of any portion of the Ethernet frame. Separate filter patterns may be defined for bridged frames, IP routed frames, and IPX routed frames.

For more information on filtering, please refer to the Programmable Filtering section of the P1705 & P1730 Reference Manual located on the accompanying CD-ROM.

MAC Address Filtering

MAC address filtering is provided by three built-in functions.

The first function is “Filter if Source”; the second is “Filter if Destination.” The third function allows you to change the filter operation from “positive” to “negative.” The positive filter operation causes frames with the specified MAC addresses to be filtered. The negative filter operation causes frames with the specified MAC addresses to be forwarded.

You may easily prevent any station on one segment from accessing a specific resource on the other segment; for this, “positive” filtering and the use of “Filter if Destination” would be appropriate. If you want to disallow a specific station from accessing any service, “Filter if Source” could be used.

You may easily prevent stations on one segment from accessing all but a specific resource on the other segment; for this, “negative” filtering and the use of “Forward if Destination” would be appropriate. If you want to disallow all but one specific station from accessing any service on the other segment, the use of “Forward if Source” could be used.

Pattern Filtering

Pattern filtering is provided in three separate sections: Bridge Pattern Filters, IP Router Pattern Filters, and IPX Router Pattern Filters. When the router is operating as an IP/IPX

Bridge/Router, each of the frames received is passed on to the appropriate internal section of the router. The IPX frames are passed on to the IPX router, the IP frames are passed on to the IP router, and all other frames are passed on to the bridge. Different pattern filters may be defined in each of these sections to provide very extensive pattern filtering on LAN traffic being sent to remote LANs.

Pattern filters are created by defining an offset value and a pattern match value. The offset value determines the starting position for the pattern checking. An offset of 0 indicates that the pattern checking starts at the beginning of the data frame. An offset of 12 indicates that the pattern checking starts at the 12th octet of the data frame. When a data frame is examined in its HEX format, an octet is a pair of HEX values with offset location 0 starting at the beginning of the frame. Please refer to *Appendix C - Octet Locations on Ethernet Frames* for more information on octet locations in data frames.

The pattern match value is defined as a HEX string that is used to match against the data frame. If the HEX data at the appropriate offset location in the data frame matches the HEX string of the filter pattern, there is a positive filter match. The data frame will be filtered according to the filter operators being used in the filter pattern.

The following operators are used in creating Pattern filters.

- offset Used in pattern filters to determine the starting position to start the pattern checking.

Example: 12-80 This filter pattern will match if the packet information starting at the 12th octet equals the 80 of the filter pattern.

| OR Used in combination filters when one **or** the other conditions must be met.

Example: 10-20|12-80 This filter pattern will match if the packet information starting at the 10th octet equals the 20 of the filter pattern or if the packet information starting at the 12th octet equals the 80 of the filter pattern.

& AND Used in combination filters when one **and** the other conditions must be met.

Example: 10-20&12-80 This filter pattern will match if the packet information starting at the 10th octet equals the 20 of the filter pattern and the packet information starting at the 12th octet equals the 80 of the filter pattern.

~ NOT Used in pattern filters to indicate that all packets **not** matching the defined pattern will be filtered.

Example: ~12-80 This filter pattern will match if the packet information starting at the 12th octet does not equal the 80 of the filter pattern.

to Filtering

- () brackets Used in pattern filters to separate portions of filter patterns for specific operators.

Example: 12-80&(14-24|14-32) This filter pattern will be checked in two operations. First the section in brackets will be checked and then the results of the first check will be used in the second check using the first portion of the filter pattern. If the packet information starting at the 14th octet equals 24 or 32, and the information at the 12th octet equals 80, the filter pattern will match.

Popular Filters

Shown here are some of the more commonly used pattern filters.

Bridge

Bridge pattern filters are applied to Ethernet frames that are bridged only. When the router is operating as a router, all routed frames will be unaffected by the bridge pattern filters.

IP & Related Traffic

| IP & Related Traffic | |
|----------------------|--------------------|
| Forward only | ~(12-0800 12-0806) |
| Filter | (12-0800 12-0806) |

Novell IPX Frames

| Novell IPX Frames | |
|-------------------|-------------------|
| EthernetII | (12-8137) |
| 802.3 RAW | (14-FFFF) |
| 802.2 | (14-E0E0) |
| 802.2 LLC | (14-AAAA&20-8137) |

NetBIOS & NetBEUI (Windows For Workgroups)

| NetBIOS & NetBEUI (Windows For Workgroups) | |
|--|------------|
| Filter | (14-F0F0) |
| Forward only | ~(14-F0F0) |

Banyan

| Banyan | |
|--------|-----------|
| | (12-0BAD) |
| | (12-80C4) |
| | (12-80C5) |

IP Router

IP router pattern filters are applied to IP Ethernet frames that are being routed. When the router is operating as an IP router, all IP routed frames will be checked against the defined IP router pattern filters. IP routed frames are unaffected by the bridge pattern filters and the IPX router pattern filters.

NetBIOS over TCP

| NetBIOS over TCP | |
|--------------------------|-----------|
| NETBIOS Name Service | (22-0089) |
| NETBIOS Datagram Service | (22-008A) |
| NETBIOS Session Service | (22-008B) |

Note: Uses the TCP Destination Port location

Other interesting TCP Ports

| Other interesting TCP Ports | | |
|-----------------------------|-----|--------|
| Decimal | Hex | Usage |
| 21 | 15 | FTP |
| 23 | 17 | Telnet |
| 25 | 19 | SMTP |
| 69 | 45 | TFTP |
| 109 | 6D | POP2 |
| 110 | 6E | POP3 |

Appendix A

Menu Trees

The menu trees on the following pages are a graphical representation of the hierarchy of the built-in menu system of the P1705 & P1730. Each of the menus are shown with the options of the menus being displayed below the specific menu name.

Each of the menu options shown in each of the menu trees is explained in the accompanying P1705 & P1730 VPN Menus Manual located on the accompanying CD-ROM.

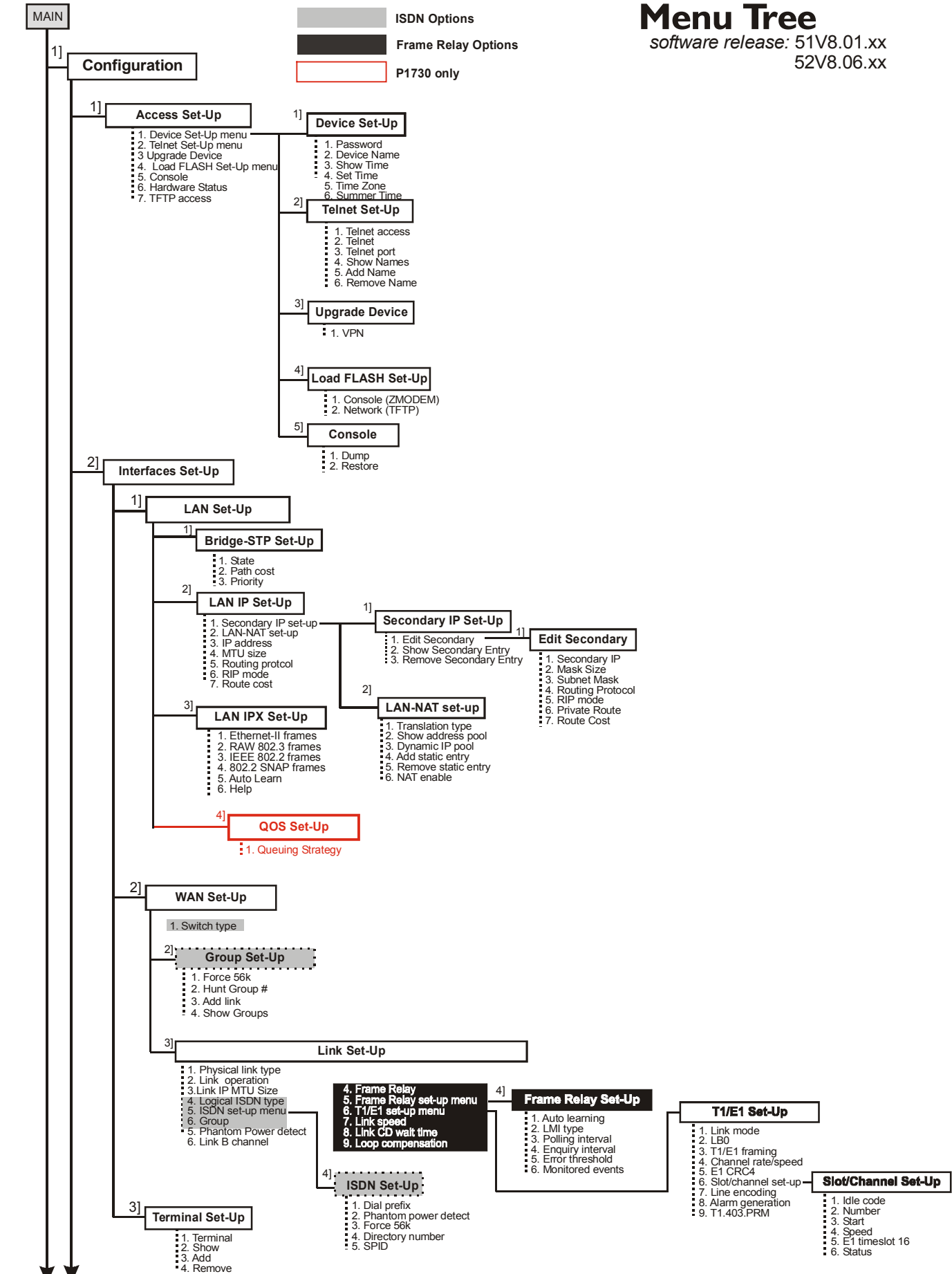
Menu names are displayed in boxes. The numbers on the left side of the boxes indicate the menu option from the parent menu that this menu corresponds to. All menu options are listed with numbers indicating their actual position within the menu system.

Menu options contained within a grayed box are ISDN options. Menu options contained within a black box are Frame Relay options.

Menu Tree

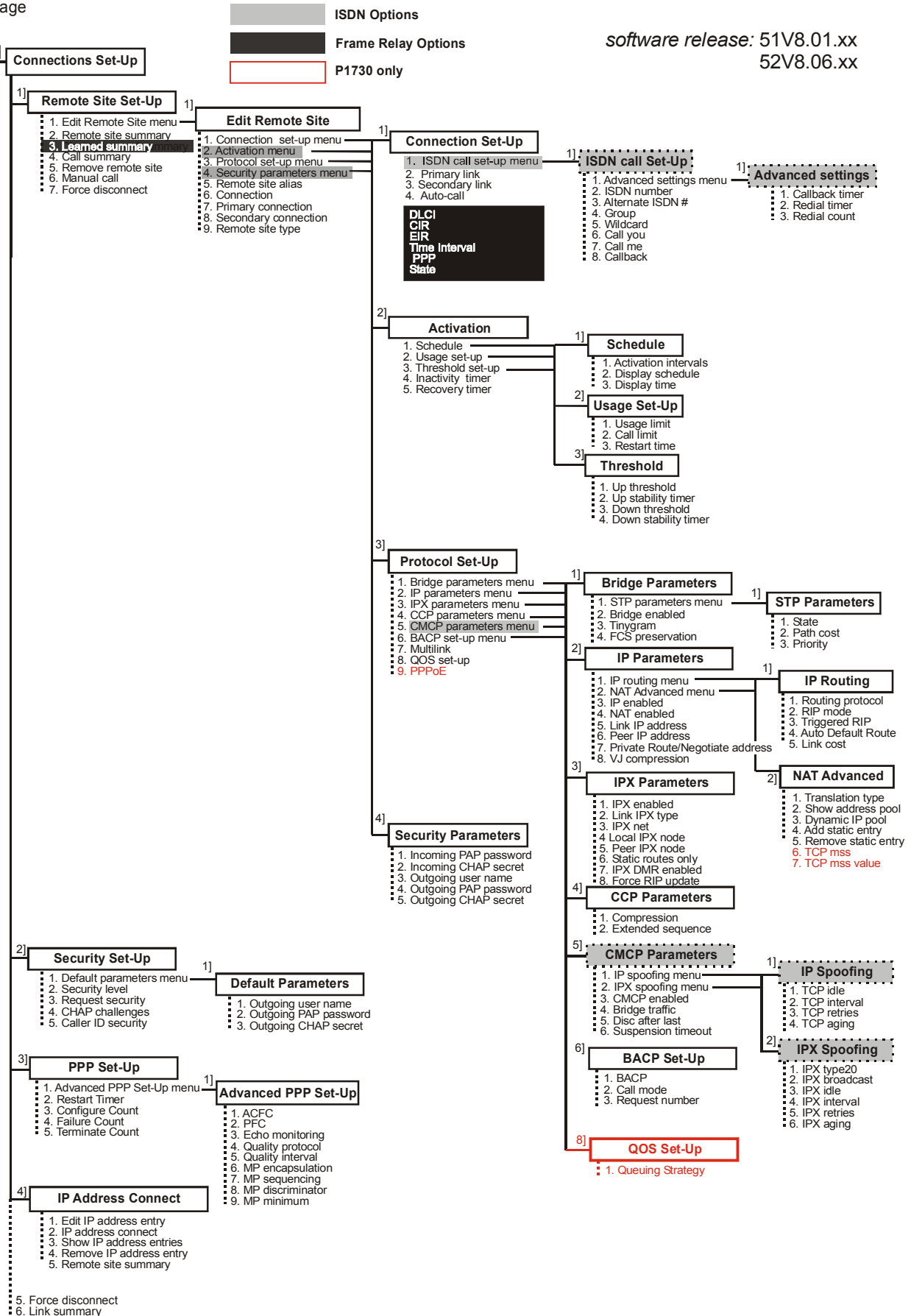
software release: 51V8.01.xx

52V8.06.xx



Continued on
next page

Continued from previous page

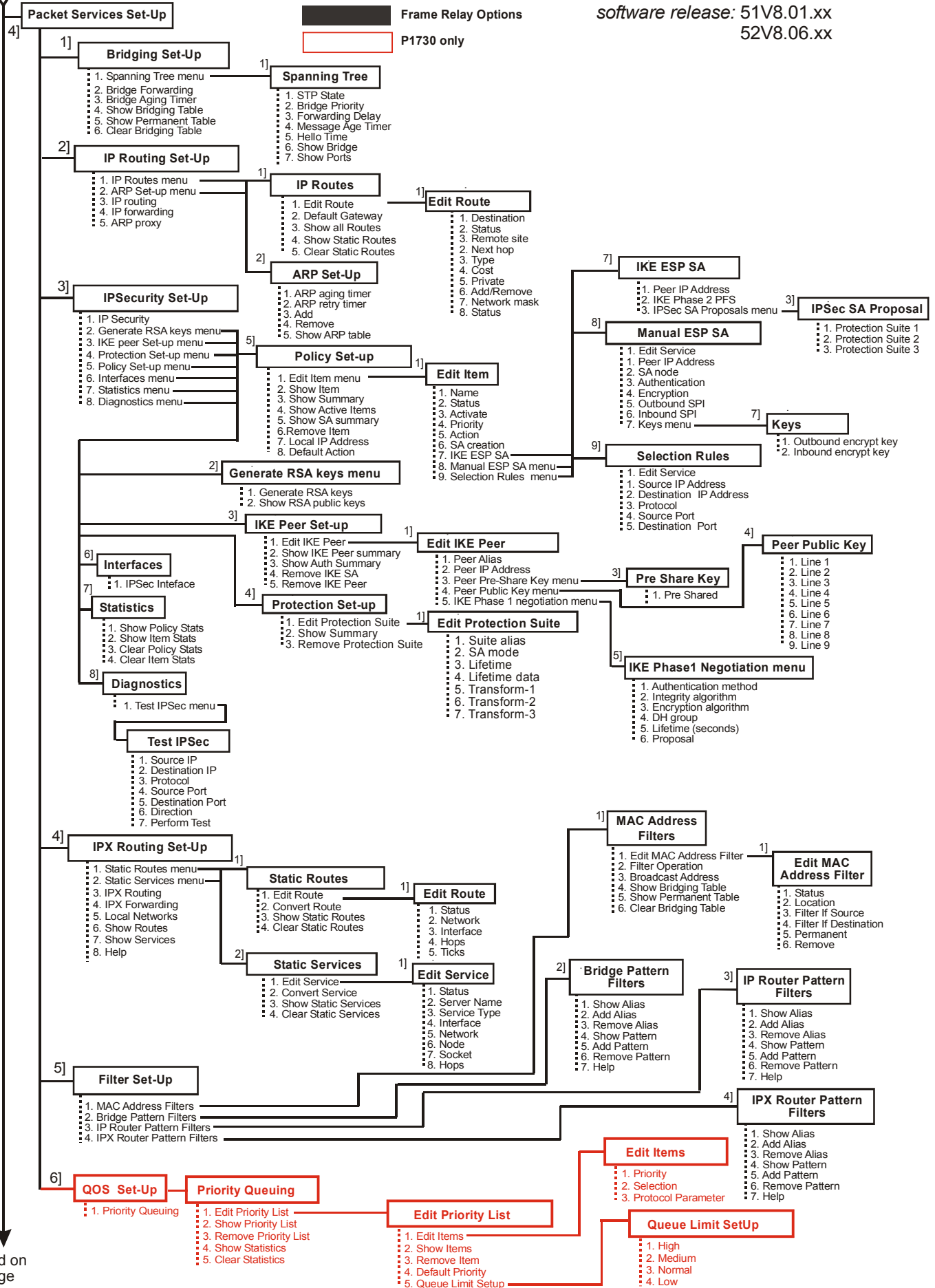


Continued on next page

continued on
next page

Frame Relay Options

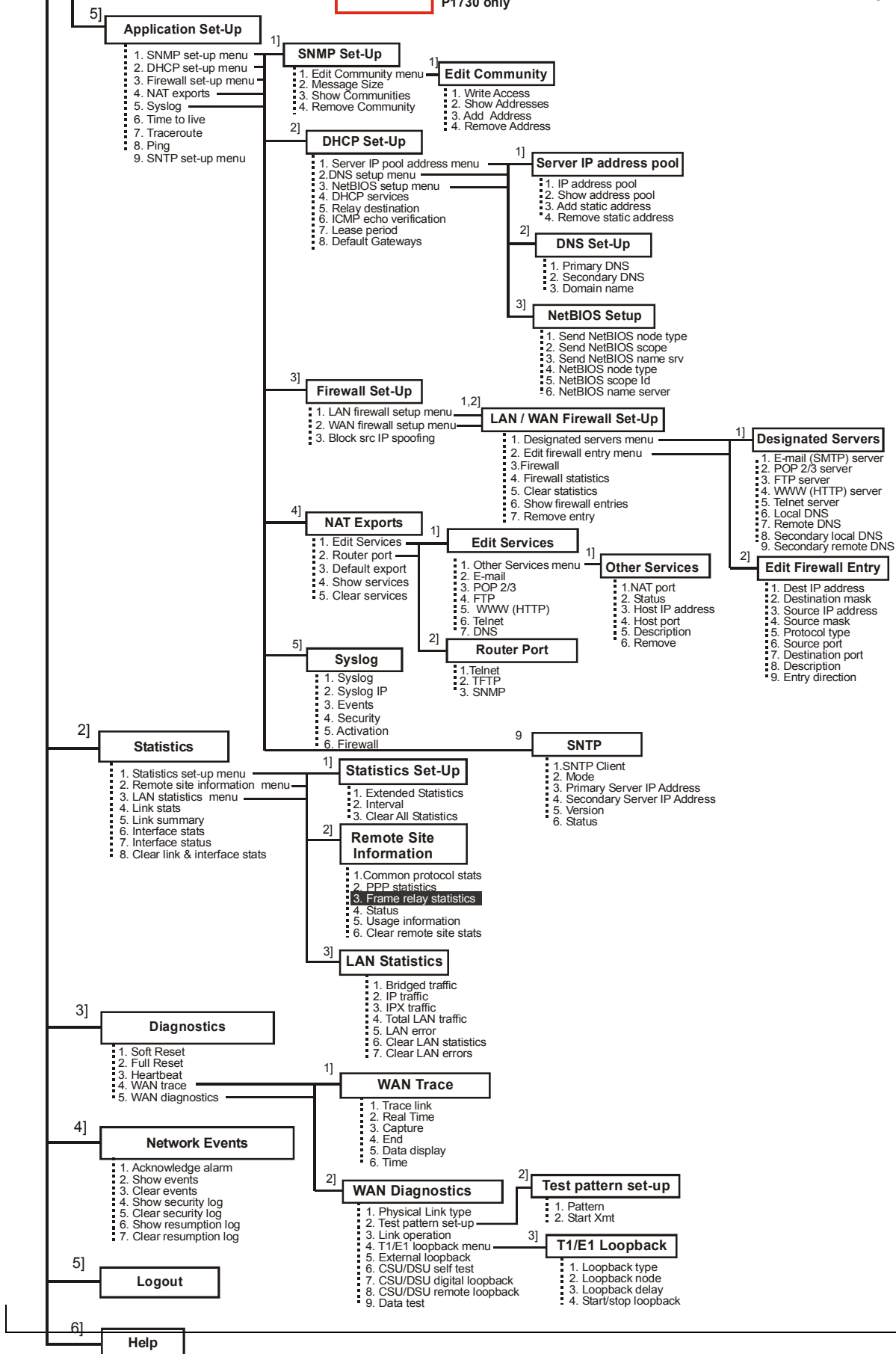
```
software release: 51V8.01.xx
                  52V8.06.xx
```



Continued from
previous page



software release: 51V8.01.xx
52V8.06.xx



Appendix B

Octet Locations on Ethernet Frames

This appendix provides octet locations for the various portions of three of the common Ethernet frames. When creating pattern filters these diagrams will assist in the correct definition of the patterns. The offset numbers are indicated by the numbers above the frame representations.

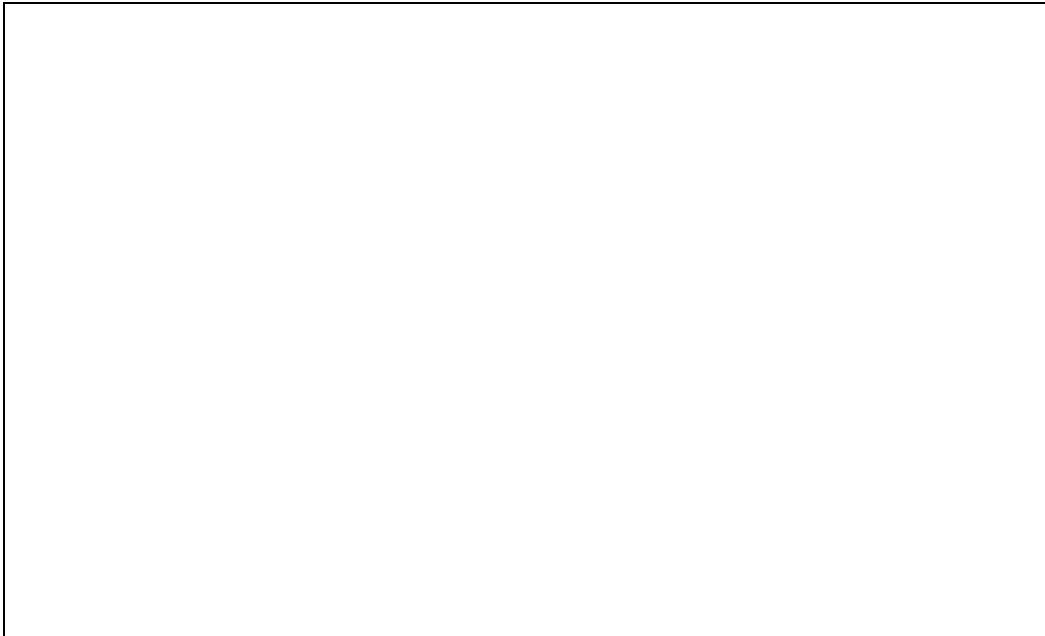
Note the differences in the TCP/IP and Novell frames when bridging and when routing. When routing, the TCP/IP and Novell frames are examined after the Level 2 Ethernet portion of the frame has been stripped from the whole data frame. This means that the offset numbers now start from 0 at the beginning of the routed frame and not the bridged frame.

Some of the common Ethernet type codes are also shown here. The Ethernet type codes are located at offset 12 of the bridged Ethernet frame.

Octet Locations on a Bridged TCP/IP Frame



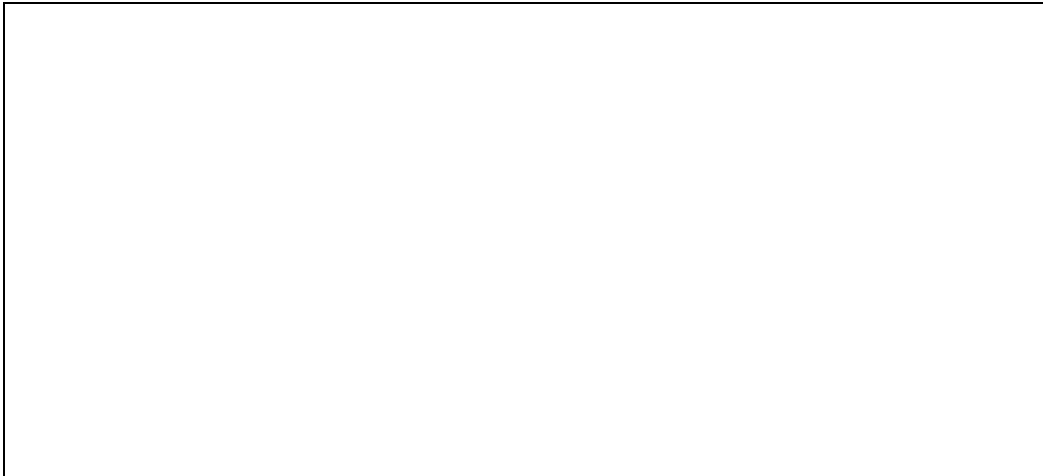
Octet Locations on a Bridged Novell Netware Frame



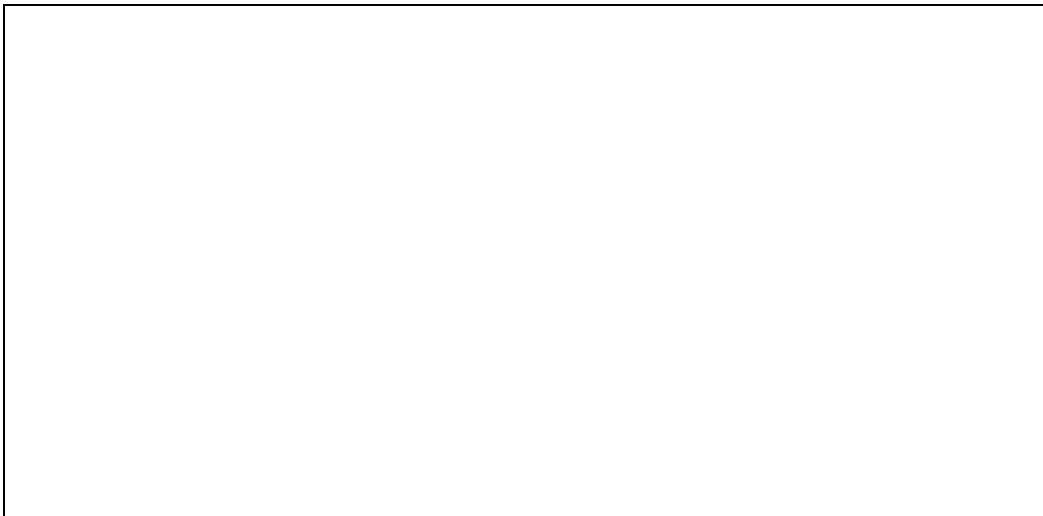
ETHERNET Type Codes

| Type Code | Description |
|-----------|---------------------------|
| 0800 | DOD IP |
| 0801 | X.75 Internet |
| 0804 | Chaosnet |
| 0805 | X.25 Level 3 |
| 0806 | ARP |
| 0807 | XNS Compatibility |
| 6001 | DEC MOP Dump/Load |
| 6002 | DEC MOP Remote Console |
| 6003 | DEC DECNET Phase IV Route |
| 6004 | DEC LAT |
| 6005 | DEC Diagnostic Protocol |
| 6006 | DEC Customer Protocol |
| 6007 | DEC LAVC, SCA |
| 8035 | Reverse ARP |
| 803D | DEC Ethernet Encryption |
| 803F | DEC LAN Traffic Monitor |
| 809B | Appletalk |
| 80D5 | IBM SNA Service on Ether |
| 80F3 | AppleTalk AARP (Kinetics) |
| 8137-8138 | Novell, Inc. |
| 814C | SNMP |

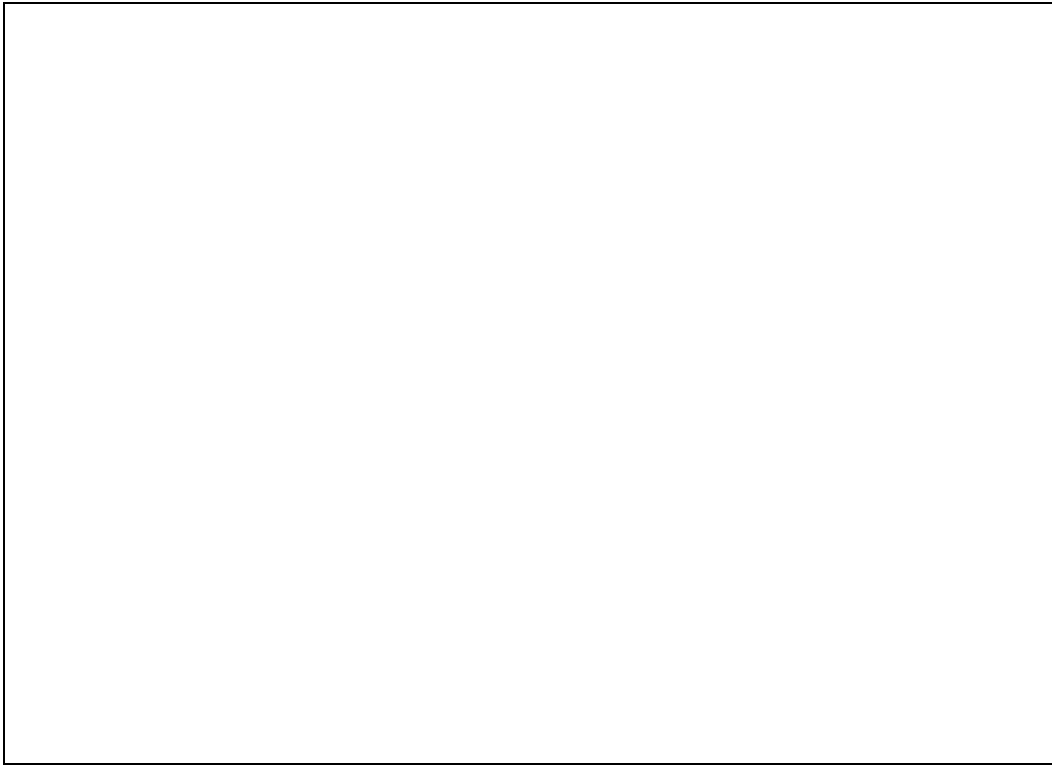
Octet Locations on an IP Routed TCP/IP Frame



Octet Locations on an IPX Routed Novell Netware Frame



Octet Locations on a Bridged XNS Frame



Appendix C

Servicing Information

Opening of the case and changing of modules is only to be performed by qualified service personnel.

WARNING !

Always disconnect the power cord from the rear panel of the bridge/router.

The bridge/router case does **not** need to be opened to change LAN or WAN interface modules.

Opening the case

- 1) Remove power from the bridge/router and remove the other cabling.
- 2) Turn the bridge/router over and place it on a flat, cushioned surface.
- 3) Remove the six Phillips head screws that fasten the case together (4 across the front and 1 on each rear side).
- 4) Hold the two halves of the case together and turn the bridge/router right-side up.
- 5) Lift off the top half of the case. The LEDs in the front panel of the bridge/router are connected to the main board by a short ribbon cable. When lifting the top half of the case off, the lid should be lifted from the back and hinged at the front. The lid will then fold completely over and lie top down.

Identifying the Internal Components

The major components of concern are shown in the following illustration.

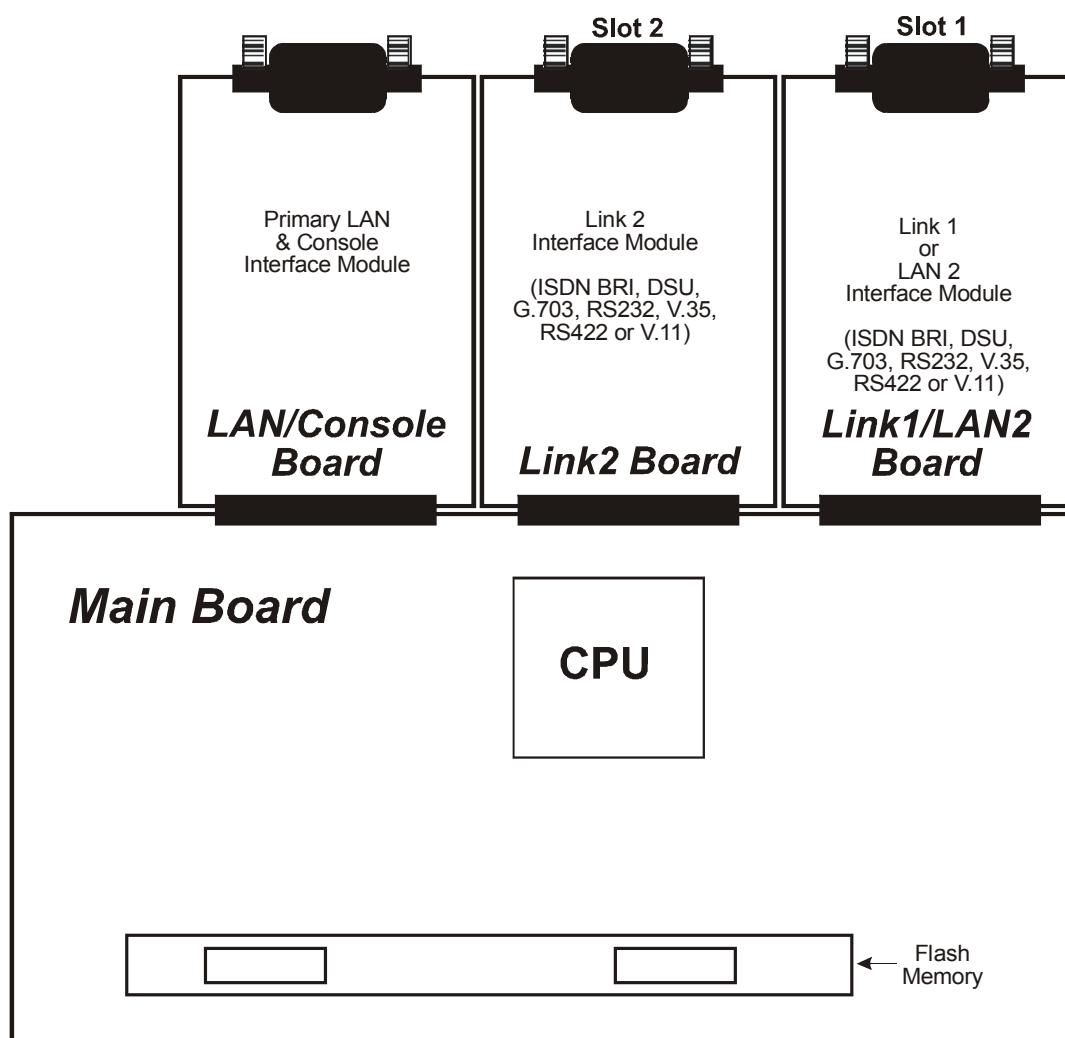


Figure C-1 Top Internal View of the P1705 & P1730 Ethernet Bridge/Router

To Clear a “Lost” Password

- 1) Remove power from the bridge/router.
- 2) Remove the screw securing the LAN / Console module to the rear of the bridge/router. Be sure to grip the module only by the flange at the bottom of the metal panel.
- 3) Unplug the LAN / Console module approximately 1/2 inch from the bridge/router. Be sure to grip the module only by the flange at the bottom of the metal panel. The module only needs to be removed slightly to disconnect the module from the internal main board.

WARNING:

Because of the close proximity of the AC power from the power coupler, do not insert anything into the LAN / Console opening while the bridge/router is powered up.

- 4) Reattach the power to the bridge/router and wait for the power-up diagnostics to finish. The Power LED will turn green.
- 5) Remove power from the bridge/router.
- 6) Re-install the LAN / Console module and secure it with the screw.
- 7) Power up the bridge/router.
- 8) Log into the bridge/router using the default password “BRIDGE” and change the password as desired.

Changing LAN or WAN Interfaces

- 1) Remove power from the bridge/router.
- 2) Remove the screw securing the interface module to the rear of the bridge/router.
- 3) Remove the interface module from the bridge/router. Be sure to grip the module only by the flange at the bottom of the metal panel.
- 4) Install the new interface module and secure it with the screw.
- 5) Power up the bridge/router.

Important: *there must be a module in slot 1 (left side module position when viewed from the rear of the unit) before a module in slot 2 (center position) will operate.*

For P1730 models, if a LAN 2 module is installed it must go in slot 1. Note in addition that installing a LAN 2 module will clear the IP address of LAN 1. After installing a LAN 2 module, the IP address for both LANs must be entered.

Selecting MDI or MDI-X LAN Interface

For most LANs, where a number of devices are connected via a hub, this router will be connected via the LAN cable to the MDI port. However, in locations where a single workstation is to be connector to the router, the cable from the workstation should be plugged into the MDI-X port. This eliminates the need for a hub at a remote site that has only one LAN device.

Installing the ISDN Link Modules

If there is an ISDN module plus another type of WAN interface module or if there is a single ISDN module, the ISDN U or S/T Module **must** only be installed in the **Slot 1** position. The slot 2 position may contain another type of WAN module or may be unused and covered with a blank panel. For P1730 models, if there is a second LAN module in this unit, it must go in the Slot 1 position and the ISDN module in Slot 2.

Note: the older double width type ISDN module will not fit in this device.

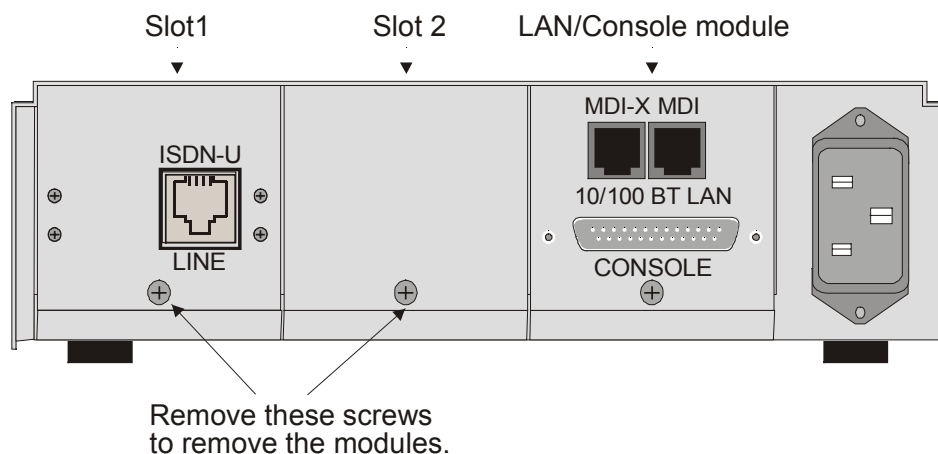


Figure C-2 Rear View with the ISDN U Module Installed

Processor settings for the ISDN Link Modules

ISDN S/T or U modules have jumper straps to set the module for the CPU used on the main board. On an S/T interface, these are labeled W1 and W2; on a U interface, the pins are labeled J1. When installing an ISDN module, check the jumpers to be certain that they are configured to operate with the 360 series CPU by having both straps across pins W1 and W2 (S/T module) or across pins 1-3 and 2-4 at J1 (U module), as illustrated in the figure below.



Figure C-4 ISDN Module processor setting jumpers

Changing the Termination Straps on the ISDN S/T Interface

The ISDN S/T link interface module has two configurable straps that control whether the ISDN LINE is set to terminated or unterminated.

Jumper straps W5 and W6 are factory installed to configure the module as **TERMINATED**. The **TERMINATED** position is used when the bridge/router is the only ISDN device connected to the ISDN circuit.

Removing the W5 and W6 straps sets the module to **UNTERMINATED**. This allows this bridge/router to be part of a daisy-chain connection to the ISDN circuit by using the ISDN AUX connector.

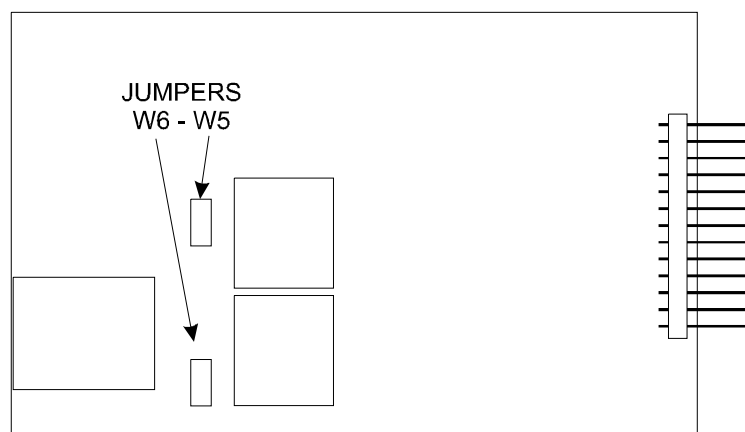


Figure C-5 ISDN S/T Module Termination setting jumpers

Connecting to the ISDN-U Link Module

The connection to the central office is made with the RJ45 connector on the panel of the U Module. Pins 4 and 5 are used for the connection. These pins are polarity insensitive.

The Ferrite module included with the ISDN U Module **must** be installed on the cable that is connected to the ISDN U Module. The Ferrite module must be installed approximately two inches from the RJ45 connector at the bridge/router end of the cable. The cable must pass through the Ferrite module twice with a Single loop around the Ferrite module.

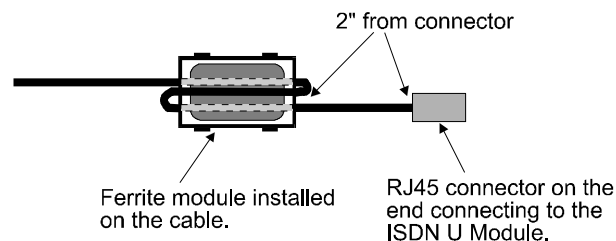


Figure C-6 Ferrite Module Installed on the Cable.

Performing a Software Upgrade

- 1) Execute the Network (TFTP) command from the Load FLASH Set-Up menu.
- 2) Enter “none” to connect locally or enter the remote site ID number or alias to connect to a remote site.
- 3) Start the TFTP application to be used for transfers to the router. (The IP address of the router may be found in the Internet Set-Up menu.).
- 4) Put the file “###.all” to the router from the Operational Code directory on the CD-ROM.

(Any router not in Network Load BOOT mode will respond with an access violation error.)

- 5) The router will verify the file “###.all” in memory, program and verify the FLASH, clear the configuration to default values (except: IP Address, IP Routing state, IP Forwarding state, WAN Environment, Link 1 & 2 State, the Switch Type, Directory Numbers, SPIDs, Password and connection data for the remote site, if applicable), and then reset. After the reset, the router will operate normally using the newly upgraded software. In some upgrade situations the Directory Numbers and SPIDs may be corrupted after the upgrade and will need to be re-entered.

- The router may take up to two (2) minutes to program and verify the FLASH. The console will not respond during this time.

To check on the router’s current state during this process, get the file “status.txt” from the router. This file will report the router’s state: both the mode and version if no errors have occurred, or an error message.

On the rare occasion that during the programming of the FLASH something happens to the bridge/router (power hit or hardware reset), causing the FLASH to become corrupted, the bridge/router will restart in ZMODEM receive mode only. If the bridge/router does not start in ZMODEM receive mode: power down the bridge/router, remove the WAN module(s) and, if present, the second LAN module, power up the bridge/router. The bridge/router should now restart and be in ZMODEM receive mode. Once the file transfer is complete, the router will again come up in ZMODEM receive mode. Power down the unit and replace the interface modules.

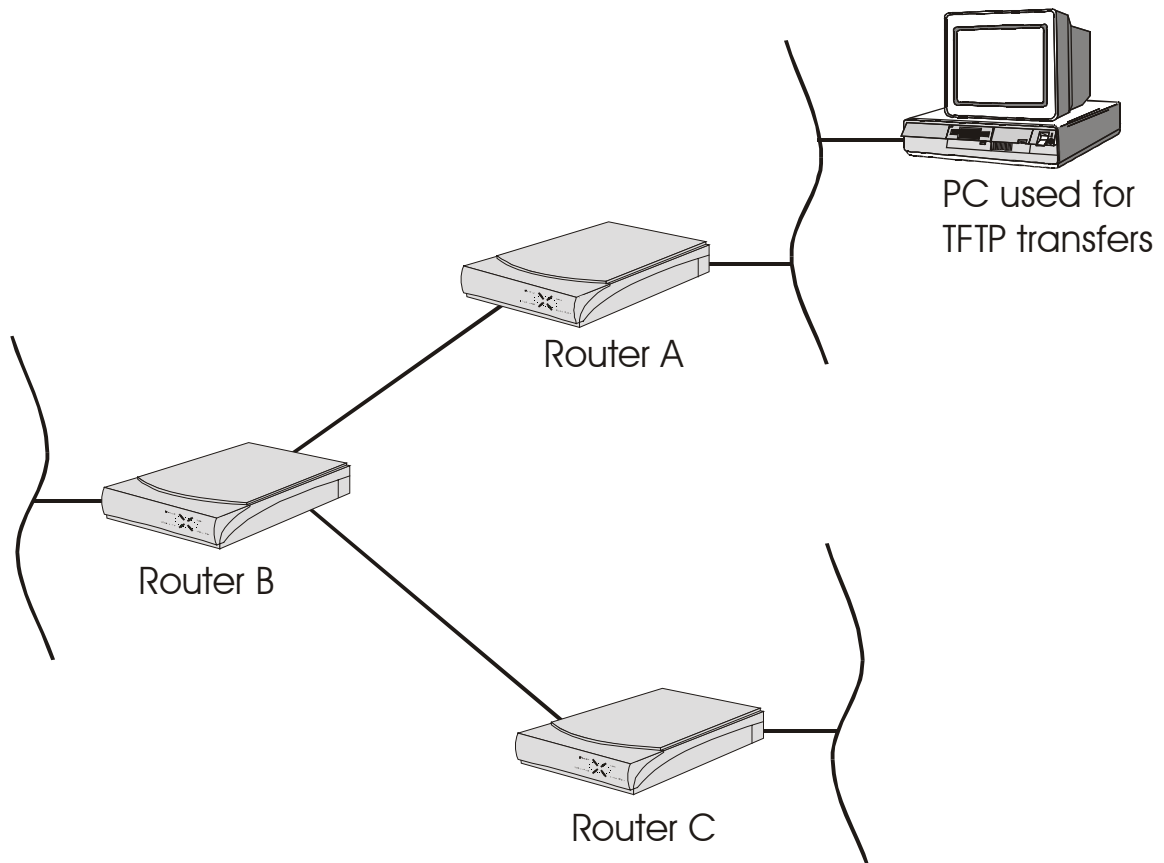
In the following diagram of a cluster of routers, when upgrading the three routers in the diagram, the upgrade order should be Router C, then Router B, and finally Router A.

A TFTP software load to router C would be performed as follows:

- Using TFTP, get config.txt from each router and save.
- Telnet to Router C. Enter the ID or alias of Router B in the Network (TFTP) option to put Router C in Network Load mode. When Router C restarts in Network Load mode, the connection to “Router B” will be re-established only if autocall is enabled on router B.
- The TFTP transfer of the upgrade code may now be performed from the PC to Router C. Once Router C has completed programming the flash and has restarted in operational mode, the connection to Router B will be re-established only if autocall is enabled on router B.

Once router C is operating with the new software, the PC may be used to reload the config.txt file back to Router C.

Repeat for Router B, then again for Router A. Perform the Router B upgrade using the ID or alias of Router A. Router A upgrades would not require a remote site ID as the PC used for TFTP transfers is located on the same LAN as Router A.



Appendix D

Interface Pinouts

Pinout Information

Each link interface available is described with detailed information on pin designation. Standard interface cables will provide correct connections to modems, datasets, or DSU/CSUs.

When connecting two bridge/routers back-to-back without modems, a null-modem cable is required to crossover the pins on the links. Crossing over the pins allows two bridge/routers both configured as DTE interfaces to be connected together. With this configuration, both bridge/routers will provide clocking for the links, and each bridge/router must have a link speed defined.

Link Clocking Information

All of the link interfaces on the router act as DTE devices, this means that they may be directly connected to DCE devices (modems, etc.) with the DCE devices providing the clocking for the link. The link speed is controlled by the DCE device. Setting the link speed on the router will not result in a speed change on the link.

Some DCE devices allow the DTE devices connected to them to supply a clock signal which is then routed back to the transmit clock pins on the DCE interface. This clock is then received by the router link interface. By using this method, the router may be in control of the link speed. The link speed may also be controlled by the router when a null-modem cable is used to connect two routers in a back-to-back configuration.

Changing the link speed within the menu system of the router changes the clock output speed that is generated on the DTE Terminal Timing pins (external clocking pins) on the link interfaces.

ATL-CSU/DSU Link Module Information

The P1705 & P1730 are currently produced with LXT CSU/DSU interface modules; however, the earlier model ATL CSU/DSU module is still compatible with the router and may be used with it. Note that ATL master mode signaling is not compatible with the current standard 64K master mode signaling; therefore, for back to back connections, an ATL unit will only operate at 64K when connected to another ATL unit. If one interface is an ATL unit and the other is not, back to back operation must be set to 56K.

The ATL-CSU/DSU link module is normally configured to receive clock from the connected network. When two ATL-CSU/DSU link modules are to be used on a leased line in a back-to-back set-up, one of the modules must provide the clock.

These modules may have either the UP/DOWN switch type or the ON/OFF slide switch type. Each type is illustrated below.

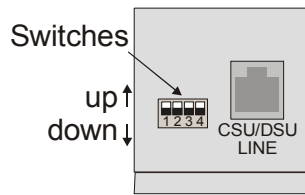


Figure D-1 Rear View of ATL-CSU/DSU Link Module with UP/DOWN Switches

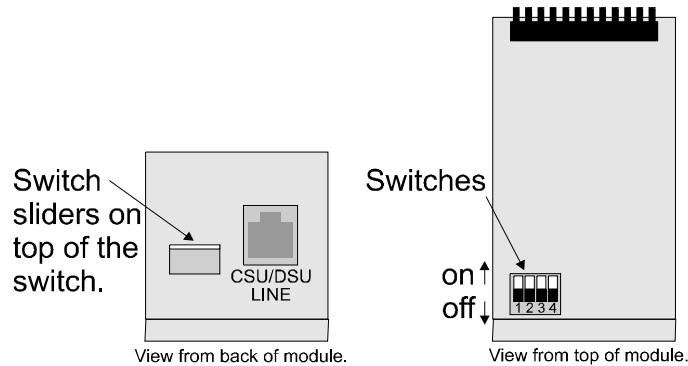


Figure D-2 View of ATL-CSU/DSU Link Module with Sliding ON/OFF Switches

When connecting two bridge/routers back-to-back with CSU/DSU link modules, a null-modem cable is required to crossover the pins on the links. Crossing over the pins allows two bridge/routers both configured as DTE interfaces to be connected together.

Switch number 1 determines whether the ATL-CSU/DSU link module will generate clocks or receive clocks. When switch 1 is down (on), the normal position, the module receives clock signals from the connected network. When switch 1 is up (up), the module will generate clocks. When a pair of routers are connected back-to-back with CSU/DSU link modules one module must be set to generate clocks and one module must be set to receive clocks.

On 64 Kbps units only, switch number 3 determines the mode of the ATL-CSU/DSU. When switch 3 is down (on), the ATL-CSU/DSU is in DDS (Digital Data Service) mode for normal connection to the 64 Kbps digital service. When switch 3 is up (off), the ATL-CSU/DSU is in LDM (Limited Distance Modem) mode for back-to-back connection with a null-modem cable.

On 56 Kbps units, the position of switch 3 is not a factor for back-to-back connection with a null-modem cable. Switch 1 must still be set as noted above.

A DSU/CSU crossover cable would be constructed as follows: 1 --> 7

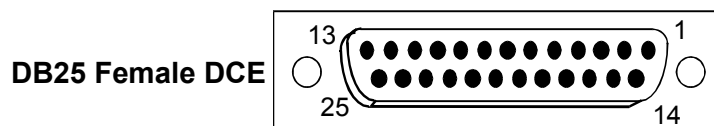
2 --> 8

7 --> 1

8 --> 2

Console Pinouts

The connector shown here and pinouts described here correspond to the connector labeled “Console” on the back of the P1705 & P1730.



| Contact Number | CCITT Circuit Number | IEEE Circuit Desig. | Circuit Name | Direction To From DCE DCE | |
|----------------|----------------------|---------------------|------------------------------------|---------------------------|---|
| 1 | 101 | AA | Protective Ground | NA | |
| 2 | 103 | BA | Transmitted Data | X | |
| 3 | 104 | BB | Received Data | | X |
| 5 | 106 | CB | Clear to Send | | X |
| 6 | 107 | CC | Data Set Ready | | X |
| 7 | 102 | AB | Signal Ground | NA | |
| 8 | 109 | CF | Received Line Signal Detector (CD) | | X |
| 20 | 108.2 | CD | Data Terminal Ready | X | |
| 22 | 125 | CE | Ring Indicator | | X |

Figure D-3 Console Pinouts

The connecting cable must be a shielded cable.

When connecting the router console directly to a modem, a null modem cable must be used because both the router console and the modem are DCE devices. A null modem cable with pinouts according to the following figure must be used.

| router Contact Number | Modem Contact Number |
|-----------------------|----------------------|
| 8 | 20 |
| 3 | 2 |
| 2 | 3 |
| 20 | 8 |
| 7 | 7 |
| 4 | 5 |
| 5 | 4 |
| 22 | 22 |

Figure D-4 Console Null Modem Cable Pinouts

T1/E1 Module:

The T1/E1 interface module use a standard RJ45 service connector, pinout specification RJ48C.

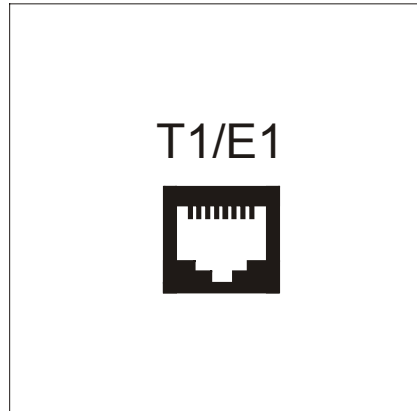


Figure D-5 Rear View of the T1/E1 Connector

When two T1/E1 routers are to be connected in a back to back set-up, a null-modem crossover cable used for the connection.

A T1/E1 crossover cable would be constructed as follows:

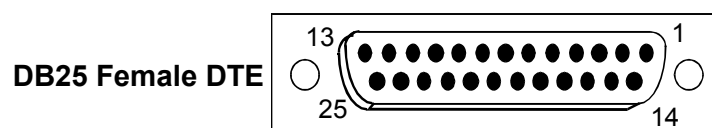
1 --> 4
2 --> 5
5 --> 2
4 --> 1

Pins 1 and 2 are receive (1 = ring, 2= tip)

Pins 4 and 5 are transmit (4 = ring, 5= tip)

V.24 & RS232C Link Pinouts

The connector shown here and pinouts described here correspond to the connector labeled “RS232 / V.24” on the back of the P1705 & P1730.



| Contact Number | CCITT Circuit Number | Circuit | Circuit Name | Direction
To From
DCE DCE | |
|----------------|----------------------|---------|---|---------------------------------|---|
| 1 | 101 | AA | Protective Ground | NA | |
| 2 | 103 | BA | Transmitted Data | X | |
| 3 | 104 | BB | Received Data | | X |
| 4 | 105 | CA | Request to Send | X | |
| 5 | | | ----- | | |
| 6 | 107 | CC | Data Set Ready | | X |
| 7 | 102 | AB | Signal Ground | NA | |
| 8 | 109 | CF | Received Line Signal Detector (CD) | | X |
| 9 | | | ----- | | |
| 10 | | | ----- | | |
| 11 | | | ----- | | |
| 12 | | | ----- | | |
| 13 | | | ----- | | |
| 14 | | | ----- | | |
| 15 | 114 | DB | Transmit Signal Element Timing (DCE Source) | | X |
| 16 | | | ----- | | |
| 17 | 115 | DD | Receive Signal Element Timing (DCE Source) | | X |
| 18 | 141 | | Local Loopback | X | |
| 19 | | | ----- | | |
| 20 | 108.2 | CD | Data Terminal Ready | X | |
| 21 | | | ----- | | |
| 22 | 125 | CE | Ring Indicator | | X |
| 23 | | | ----- | | |
| 24 | 113 | DA | Transmit Signal Element Timing (DTE Source) | X | |
| 25 | | | ----- | | |

Figure D-5 RS232 Link Pinouts

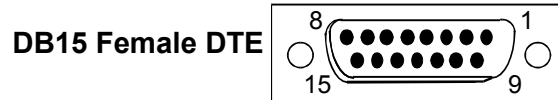
The connecting cable must be a shielded cable.

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M. Each end must be terminated in a male 25 pin X.21 bis connector as defined in ISO-2110 1989.

V.11/X.21 Link Pinouts

The connector shown here and pinouts described here correspond to the connector labeled “V.11/x.21” on the back of the P1705 & P1730.



| Contact Number | X.21 Circuits Reference | Circuit Name | Direction | |
|----------------|-------------------------|---------------------------|-----------|----------|
| | | | To DCE | From DCE |
| 1 | | Protective Ground | NA | |
| 2 | T (A) | Transmitted Data (A) | X | |
| 3 | C (A) | Control (A) | X | |
| 4 | R (A) | Received Data (A) | | X |
| 5 | I (A) | Indication (A) | | X |
| 6 | S (A) | Signal Element Timing (A) | | X |
| 7 | | ----- | | |
| 8 | Ground | Signal Ground | NA | |
| 9 | T (B) | Transmitted Data (B) | X | |
| 10 | C (B) | Control (B) | X | |
| 11 | R (B) | Received Data (B) | | X |
| 12 | I (B) | Indication (B) | | X |
| 13 | S (B) | Signal Element Timing (B) | | X |
| 14 | | ----- | | |
| 15 | | ----- | | |

Figure D-6 V.11/x.21 Link Pinouts

The connecting cable must be a shielded cable.

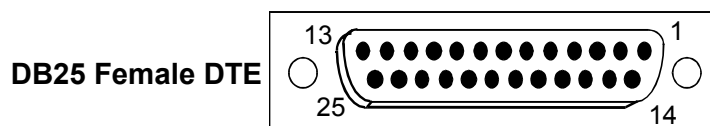
Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M. Each end must be terminated in a male 15 pin X.21 connector as defined in ISO-4903 1989, but one end of the cable must have UNC-4-40 screws and the other end must have M3 screws.

RS442 & RS530 Link Pinouts

The connector shown here and pinouts described here correspond to the connector labeled “RS530” on the back of the P1705 & P1730.



| Contact Number | Circuit | Circuit Name | Direction
To From
DCE DCE | |
|----------------|---------|---|---------------------------------|---|
| 1 | Shield | Protective Ground | NA | |
| 2 | BA (A) | Transmitted Data | X | |
| 3 | BB (A) | Received Data | | X |
| 4 | CA (A) | Request to Send | X | |
| 5 | CB (A) | Clear to Send | | X |
| 6 | CC (A) | Data Set Ready | | X |
| 7 | AB | Signal Ground | NA | |
| 8 | CF (A) | Received Line Signal Detector | | X |
| 9 | DD (B) | Receive Signal Element Timing (DCE Source) | | X |
| 10 | CF (B) | Received Line Signal Detector | | X |
| 11 | DA (B) | Transmit Signal Element Timing (DTE Source) | X | |
| 12 | DB (B) | Transmit Signal Element Timing (DCE Source) | | X |
| 13 | CB (B) | Clear to Send | | X |
| 14 | BA (B) | Transmitted Data | X | |
| 15 | DB (A) | Transmit Signal Element Timing (DCE Source) | | X |
| 16 | BB (B) | Received Data | | X |
| 17 | DD (A) | Receive Signal Element Timing (DCE Source) | | X |
| 18 | LL | Local Loopback | X | |
| 19 | CA (B) | Request to Send | X | |
| 20 | CD (A) | Data Terminal Ready | X | |
| 21 | RL | Remote Loopback | X | |
| 22 | CC (B) | Data Set Ready | | X |
| 23 | CD (B) | Data Terminal Ready | X | |
| 24 | DA (A) | Transmit Signal Element Timing (DTE Source) | X | |
| 25 | | ----- | | |

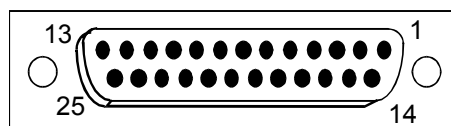
Figure D-7 RS530 Link Pinouts

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

V.35 Link Pinouts

The connector pinouts described here correspond to the connector labeled “V.35” on the back of the P1705 & P1730.



| DB25
Contact
Number | M.34
Contact
Number | Circuit
Name | <u>Direction</u> | |
|---------------------------|---------------------------|--|------------------|-------------|
| | | | To
DCE | From
DCE |
| 1 | A | Protective Ground | NA | |
| 2 | | ----- | | |
| 3 | | ----- | | |
| 4 | C | Request to Send | X | |
| 5 | | ----- | | |
| 6 | E | Data Set Ready | | X |
| 7 | B | Signal Ground | NA | |
| 8 | F | Data Channel Received Line Signal Detector | | X |
| 9 | P | Transmitted Data (A) | X | |
| 10 | S | Transmitted Data (B) | X | |
| 11 | R | Received Data (A) | | X |
| 12 | T | Received Data (B) | | X |
| 13 | | ----- | | |
| 14 | V | Receiver Signal Element Timing (A) | | X |
| 15 | | ----- | | |
| 16 | X | Receiver Signal Element Timing (B) | | X |
| 17 | | ----- | | |
| 18 | U | Transmitter Signal Element Timing (A) DTE | X | |
| 19 | W | Transmitter Signal Element Timing (B) DTE | X | |
| 20 | H | Data Terminal Ready | X | |
| 21 | | Local Loopback | X | |
| 22 | J | Calling Indicator | | X |
| 23 | Y | Transmitter Signal Element Timing (A) | | X |
| 24 | | ----- | | |
| 25 | a | Transmitter Signal Element Timing (B) | | X |

Figure D - 8 V.35 Link Pin Outs

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

NOTE For U.K. Approval:

The connecting cable may be any length between 0 and 5M. One end must be terminated in a male 34 pin X.21 bis connector as defined in ISO-2593 1984. The other end must be terminated in a male 25 pin X.21 bis connector as defined in ISO-2110 1989

RS232 Null-Modem Cable Configuration

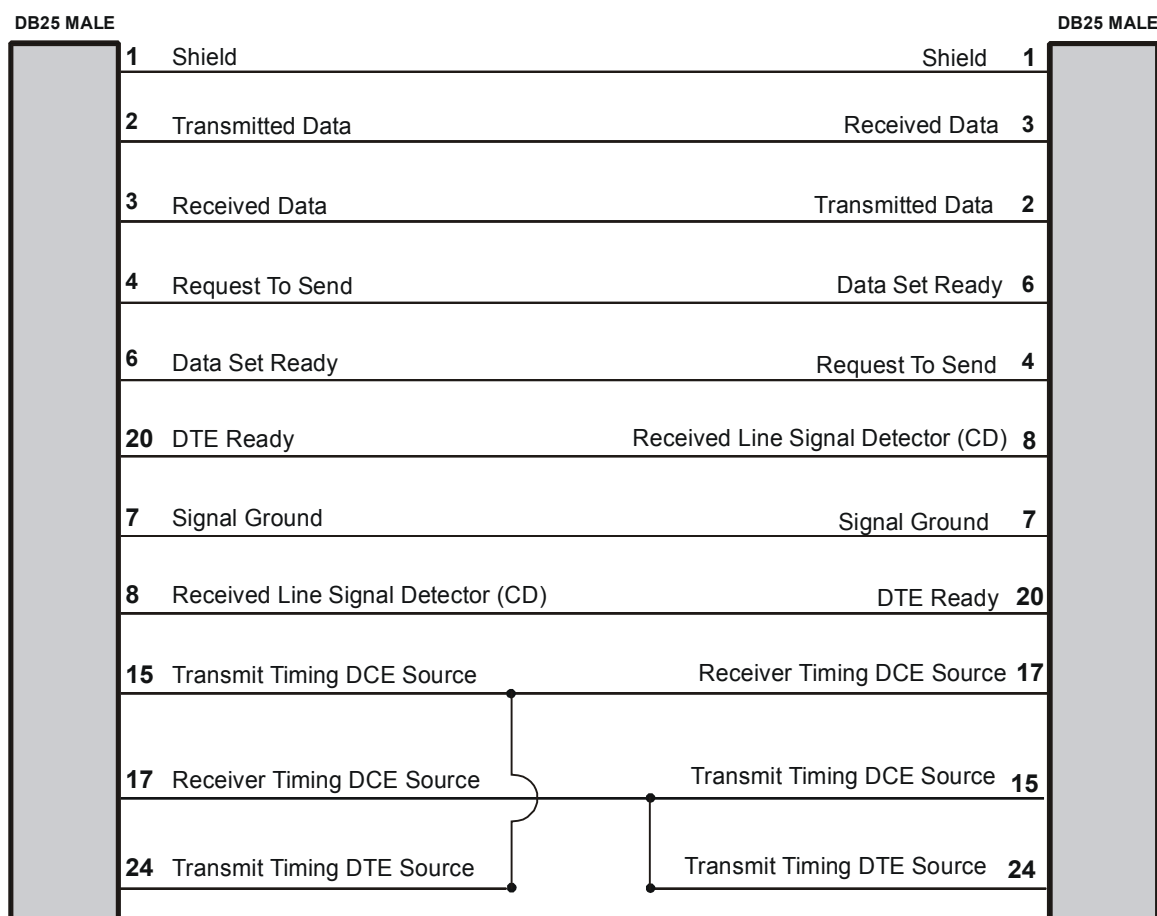


Figure D-9 RS232 Null-Modem Cable

The connecting cable must be a shielded cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB25 connectors on each end to allow direct connection to the link interface connector on each unit. The link speed must be defined for each of the two units.

V.35 Null-Modem Cable Configuration

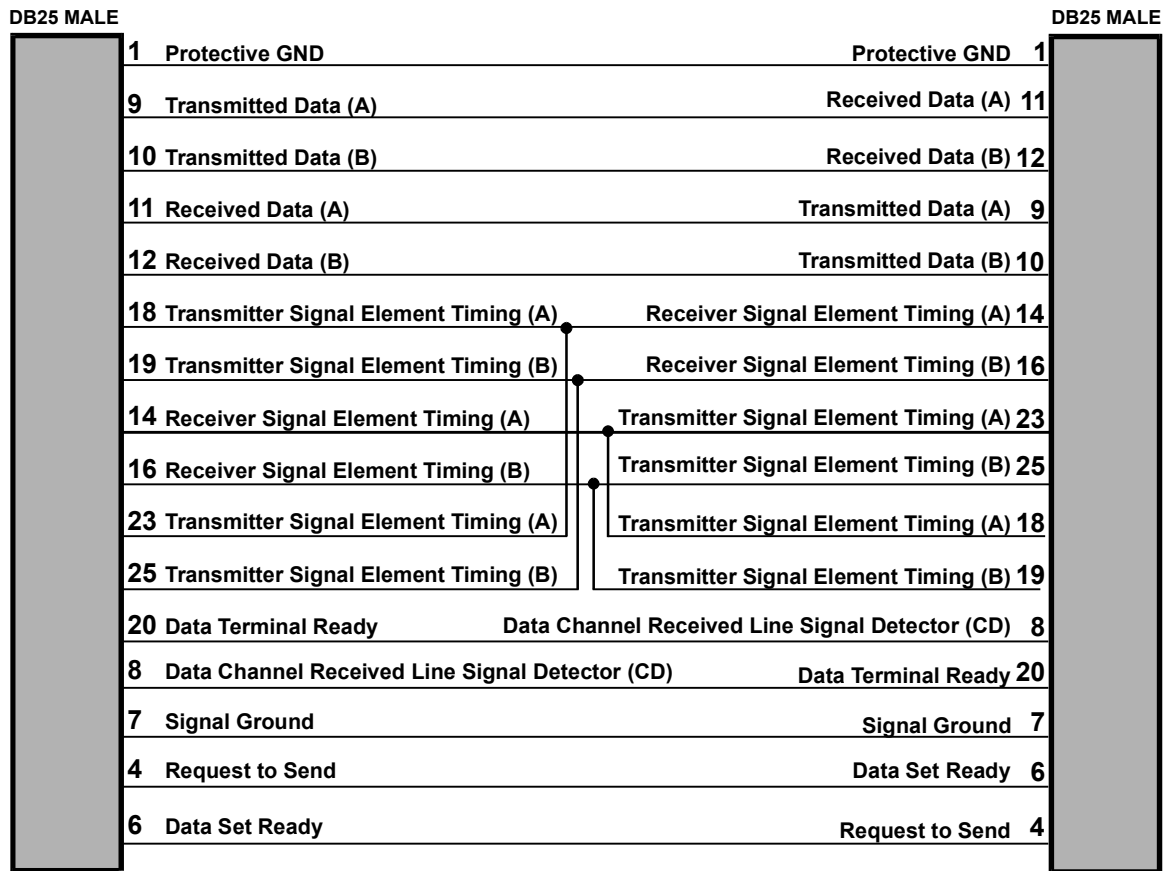


Figure D – 10 V-35 Null-Modem Cable

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB25 connectors on each end to allow direct connection to the link interface connector on each unit.

The link speed must be defined for each of the two units.

RS530 Null-Modem Cable Configuration

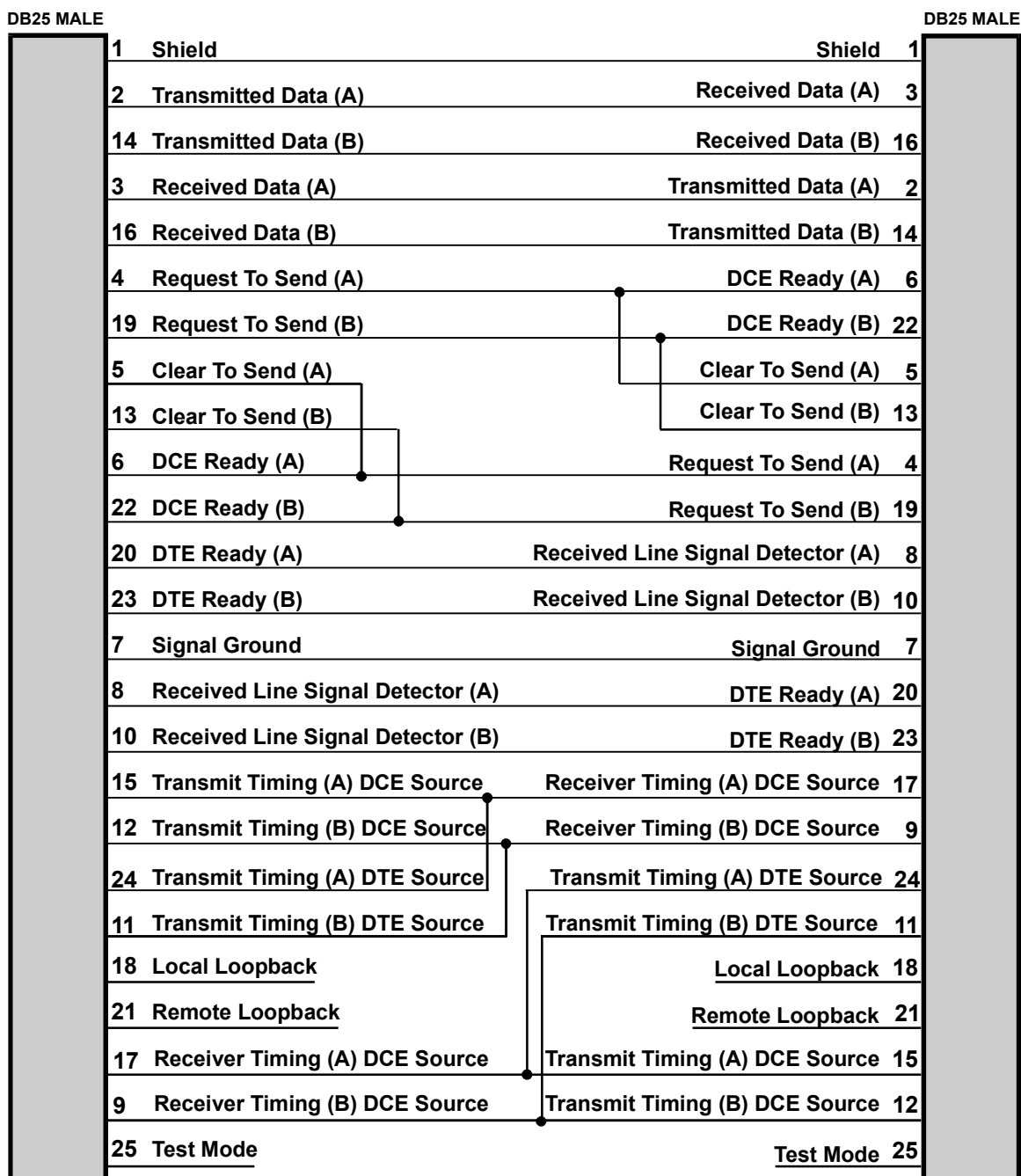


Figure D-11 RS530 Null-Modem Cable

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB25 connectors on each end to allow direct connection to the link interface connector on each unit. The link speed must be defined for each of the two units.

RS530 To RS449 Conversion Cable

| DB25 MALE | | DB37 MALE/FEMALE |
|-----------|---|------------------|
| 2 | Transmitted Data (A) | 4 |
| 14 | Transmitted Data (B) | 22 |
| 3 | Received Data (A) | 6 |
| 16 | Received Data (B) | 24 |
| 8 | Received Line Signal Detector (A) | 13 |
| 10 | Received Line Signal Detector (B) | 31 |
| 6 | Data Set Ready (A) | 11 |
| 22 | Data Set Ready (B) | 29 |
| 4 | Request to Send (A) | 7 |
| 19 | Request to Send (B) | 25 |
| 5 | Clear to Send (A) | 9 |
| 13 | Clear to Send (B) | 27 |
| 20 | Data Terminal Ready (A) | 12 |
| 23 | Data Terminal Ready (B) | 30 |
| 17 | Receiver Signal Element Timing (DCE Source) (A) | 8 |
| 9 | Receiver Signal Element Timing (DCE Source) (B) | 26 |
| 15 | Transmit Signal Element Timing (DCE Source) (A) | 5 |
| 12 | Transmit Signal Element Timing (DCE Source) (B) | 23 |
| 24 | Transmit Signal Element Timing (DTE Source) (A) | 17 |
| 11 | Transmit Signal Element Timing (DTE Source) (B) | 35 |
| 7 | Signal Ground | 19 |
| 1 | Shield | 1 |

Figure D-12 RS530 to RS449 Conversion Cable

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

This cable is used to connect an RS530 link to an RS449 device. The cable converts from a DB25 connector to a DB37 connector.

V.11/X.21 Null-Modem Cable Configuration

| DB15 MALE | | | | DB15 MALE |
|-----------|----|---------------------------|---------------------------|-----------|
| | 1 | Protective Ground | Protective Ground | 1 |
| | 2 | Transmit Data (A) | Receive Data (A) | 4 |
| | 3 | Control (A) | Indication (A) | 5 |
| | 4 | Receive Data (A) | Transmit Data (A) | 2 |
| | 5 | Indication (A) | Control (A) | 3 |
| | 6 | Signal Element Timing (A) | Signal Element Timing (A) | 6 |
| | 7 | Not Used | Not Used | 7 |
| | 8 | Signal Ground | Signal Ground | 8 |
| | 9 | Transmit Data (B) | Receive Data (B) | 11 |
| | 10 | Control (B) | Indication (B) | 12 |
| | 11 | Receive Data (B) | Transmit Data (B) | 9 |
| | 12 | Indication (B) | Control (B) | 10 |
| | 13 | Signal Element Timing (B) | Signal Element Timing (B) | 13 |
| | 14 | Not Used | Not Used | 14 |
| | 15 | Not Used | Not Used | 15 |

Figure D-13 V.11/X.21 Null-Modem Cable

The connecting cable must be a shielded cable.

Circuits which are paired (contain an (A) and (B) reference) should be connected to twisted pairs within the connecting cable.

This cable is needed when it is necessary to connect two units back-to-back and a set of modems is not available. Note that this cable specifies DB15 connectors on each end to allow direct connection to the link interface connector on each unit. The link speed must be defined for each of the two units.

When using this cable to connect two units back-to-back, a jumper must be installed on pinheaders W8 and W9 on one of the V.11/X.27 interface modules. This allows that particular module to generate the required timing signals.